Interprétation p-automatique des groupes formels le Lubin-Tate et des modules de Drinfeld réduits

Christophe Cadic

Numéro d'ordre : 01/99 Université de Limoges

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Spécialité : Mathématiques Pures

Présentée et soutenue publiquement par

Christophe CADIC

le 14 Janvier 1999

Interprétation p-automatique des groupes formels de Lubin-Tate et des modules de Drinfeld réduits

Directeur de Thèse : François LAUBIE

JURY :

Président et Rapporteur	**Y. HELLEGOUARCH**	Professeur à l'Université de Caen
Rapporteur	**J.-P. ALLOUCHE**	Directeur de recherches au C.N.R.S. Université de Paris Sud
Rapporteur	**J.-P. WINTENBERGER**	Professeur à l'Université de Strasbourg
Examinateur	**J.-P. BOREL**	Professeur à l'Université de Limoges
Examinateur	**I. FESENKO**	Professeur à l'Université de Nottingham
Examinateur	**F. LAUBIE**	Professeur à l'Université de Limoges
Examinateur	**A. C. MOVAHHEDI**	Maître de Conférences habilité à diriger des recherches à l'Université de Limoges
Examinateur	**A. SALINIER**	Maître de Conférences à l'Université de Limoges

Remerciements

Je tiens à remercier mon directeur de thèse, François Laubie, pour l'attention qu'il a portée sur ce travail durant ces trois années ainsi que pour la disponibilité dont il a su faire part, malgré un emploi du temps très chargé.

Je remercie Jean-Paul Allouche pour le suivi régulier qu'il a apporté à cette thèse ainsi que pour les nombreuses idées que nous avons échangées. Je lui suis très reconnaissant d'avoir accepté d'être rapporteur.

Yves Hellegouarch m'a fait l'honneur d'être rapporteur et ses précieux conseils, ainsi que son expérience, me furent d'une très grande utilité. Je l'en remercie vivement.

C'est également un grand honneur pour moi que Jean-Pierre Wintenberger ait accepté d'être rapporteur et je l'en remercie.

J'exprime ma reconnaissance à Jean-Pierre Borel et Ivan Fesenko pour leur aimable participation à ce jury.

Je remercie Alain Salinier, A. Chazad Movahhedi ainsi que Véronique Mauduit pour les nombreuses discussions complémentaires que nous avons eues.

Merci enfin à Martine Guerletin, Yolande Pinol et Nadine Tchéfranoff pour leur disponibilité et leur sympathie.

Je ne saurais clôre cette page sans remercier Véronique, mon épouse, pour sa grande patience et son soutien durant ces années.

Table des matières

Introduction

Des notions telles que l'algébricité ou la rationalité d'une série sur $\mathbb{F}_q(T)$ ne semblent pas a priori avoir de rapport direct, si ce n'est que la rationalité implique l'algébricité. En fait, nous voyons dans ce travail que des applications telles que certaines lois de réciprocité associent de manière bi-univoque les éléments rationnels aux éléments algébriques.
Cette association ne fait que traduire la nature p-automatique des procédés de construction des images de ces applications.

Le chapitre 1 est un rappel des principales notions qui seront utilisées par la suite. On y retrouve la théorie des groupes formels de Lubin-Tate, la construction des corps de normes de Fontaine-Wintenberger ainsi que le lien entre les séries algébriques et les automates.
Ce chapitre se conclut par l'établissement de propriétés d'algébricité des séries. On voit comment l'algébricité se transporte via l'opération de composition.

Dans le chapitre 2, nous étudions le procédé de construction des endomorphismes des groupes formels de Lubin-Tate. L'étude particulière du groupe multiplicatif sur $\mathbb{Z}_p$ fait apparaître, avec les notations standard, que l'image $[u]_{ff}(T) = (1+T)^u - 1$ de l'élément $u \in \mathbb{Z}_p$, réduite modulo p, est algébrique sur $\mathbb{F}_p(T)$ si et seulement si l'élément u est rationnel. Ce résultat est dû entre autres à Robba dans [29] mais aussi à Mendès France et van der Poorten dans [28] ainsi qu'à Allouche, Mendès France et van der Poorten sous une forme plus générale que [28] dans [5].
On s'aperçoit alors que s'il existe des groupes formels de Lubin-Tate isomorphes sur $\mathbb{Z}_p$ au groupe multiplicatif par un isomorphisme de réduction modulo p algébrique, ils vérifient cette même propriété. On s'assure de l'existence de tels groupes en faisant appel au Lemme de l'Équation Fonctionnelle [21].
En interprétant les réductions modulo p des endomorphismes des groupes de Lubin-Tate en tant qu'automorphismes d'un corps local de caractéristique p, on s'intéresse au problème de l'algébricité des restrictions à certains sous-corps. Notons que le corps local en question est le corps de normes de l'extention A.P.F. (Arithmétiquement profinie) de $\mathbb{Q}_p$ définie par le groupe formel. Il apparaît ainsi que si la norme d'une uniformisante du corps de normes (qui est une série à coefficients dans un corps fini) est algébrique, on a l'équivalence entre la rationalité de l'élément u et l'algébricité de la série représentant la restriction issue de u. Ce cas se présente lorsque la sous-extension du corps de normes, induit un groupe de Galois isomorphe au groupe $\mu_2 = \{-1, 1\}$ des racines de 1.

On s'aperçoit ensuite que ces restrictions peuvent être vues comme étant les réductions modulo p d'endomorphismes de groupes formels, qui quant à eux ne sont plus de Lubin-Tate. On caractérise ces groupes formels en calculant leur logarithme et on donne des formules explicites des endomorphismes. Celles-ci s'obtiennent grâce aux polynômes de Bell et font intervenir les polynômes de Chebyshev dans un cas particulier.
Enfin on s'intéresse au problème de l'indépendance algébrique de ces automorphismes. On fait apparaître que leur indépendance algébrique sur $\mathbb{F}_p(T)$ est équivalente à l'indépendance linéaire sur $\mathbb{Z}$ des unités d'où ils sont issus. Nous établissons ensuite la validité de ce résultat pour les restrictions aux sous-corps induisant le groupe de Galois μ_2.
On conclut ce chapitre en établissant les équivalences dans le contexte d'un groupe formel particulier, mais qui cette fois est défini, non plus sur $\mathbb{Z}_p$, mais sur un anneau de séries formelles à coefficients dans $\mathbb{F}_p$. On démontre alors dans ce cas que la norme d'une uniformisante du corps de normes est algébrique lorsqu'elle est prise relativement à n'importe quel sous-corps. Ceci permet d'étendre l'équivalence entre la rationalité de u et l'algébricité de la restriction issue de u dans le cadre de tous les sous-corps du corps de normes formant un groupe de Galois fini.

Dans le chapitre 3, on regarde les endomorphismes du module de Carlitz formel. Ce module donnant l'analogue de l'exponentiation dans le contexte des polynômes, il est naturel de se demander s'il existe un analogue à l'assertion "$(1+T)^a$ modulo p est algébrique sur $\mathbb{F}_p(T)$ si et seulement si $a \in \mathbb{Z}_p \cap \mathbb{Q}$".
Nous établissons dans un premier temps cet analogue, à savoir : Pour $P(t) \in \mathbb{F}_q[t]$ irréductible et unitaire, la réduction modulo $P(t)$ d'un endomorphisme du module de Carlitz formel (défini sur le complété $P(t)$-adique $\mathbb{F}_q[t]_P$ de $\mathbb{F}_q[t]$) est algébrique si et seulement si cet endomorphisme est issu d'un élément $R(t)$ rationnel.
Ensuite on considère les modules de Drinfeld de rang 1. En calculant un isomorphisme avec le module de Carlitz, on établit le résultat pour ces derniers, lorsque leur réduction n'est pas triviale.
Pour conclure cette partie, on regarde la suite des coefficients des puissances de σ dans l'expression des endomorphismes d'un module de Drinfeld formel de rang 1. On établit alors une condition nécessaire et suffisante pour que la réduction modulo $P(t)$ de cette suite soit p-automatique.

Chapitre 1

Généralités

1.1 Groupes formels de Lubin-Tate

1.1.1 Définitions

Soit A un anneau commutatif. On note $A[[T]]$ l'ensemble des séries formelles $\sum_{i=0}^{\infty} a_i T^i$ à coefficients dans A. Muni de l'addition et de la multiplication classiques des séries, $A[[T]]$ devient un anneau. Si A est intègre, $A[[T]]$ l'est aussi et on représente par $A((T))$ le corps des fractions de $A[[T]]$.

Définition 1.1.1 *On dit qu'une série $a(T) \in A[[T]]$ est réversible (dans $A[[T]]$) s'il existe une série $b(T) \in A[[T]]$ telle que $a(b(T)) = b(a(T)) = T$. On note alors $b(T) = a^{-1}(T)$.*

Remarque 1 : On trouve souvent dans la littérature la notation $a^{\circ -1}(T)$ pour l'inverse de composition de $a(T)$. Nous préserverons néanmoins la notation $a^{-1}(T)$. Lorsque nous aurons affaire à l'inverse multiplicatif, le texte sera suffisamment précis de manière à ce qu'il n'y ait pas d'ambiguïté.
Remarque 2 : Une condition nécessaire et suffisante pour que $a(T) \in A[[T]]$ soit réversible est que $a(T) \equiv uT \pmod{\deg 2}$ avec u inversible dans A.

Soit K un corps local de corps résiduel fini et d'anneau des entiers A. Soit $\pi \in A$ tel que $v(\pi) = 1$ et soit q le cardinal du corps résiduel $A/\pi A$. On note

$$\mathcal{F}_\pi = \{f(T) \in A[[T]] | f(T) \equiv \pi T \pmod{\deg 2},\ f(T) \equiv T^q \pmod{\pi}\}$$

Définition 1.1.2 *On appelle groupe formel sur A une série $F(X,Y) \in A[[X,Y]]$ telle que :*

1) $F(X,Y) \equiv X + Y \pmod{\deg 2}$,

2) $F(X,Y) = F(Y,X)$,

3) $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

Exemple : On appelle "groupe additif" le groupe formel $G_a(X,Y) = X+Y$.

Définition 1.1.3 *Soient F et G deux groupes formels sur A. On appelle homomorphisme de F dans G toute série $\theta(T) \in A[[T]]$ telle que :*

$$\theta(F(X,Y)) = G(\theta(X),\theta(Y)).$$

Remarques :

1) L'ensemble des homomorphismes de F dans G se note $\mathrm{Hom}_A(F,G)$ ou $\mathrm{Hom}(F,G)$ lorsqu'il n'y a pas d'ambiguïté.

2) On emploie les notations suivantes :

- $\theta(F(X,Y)) = \theta \circ F$,
- $G(\theta(X),\theta(Y)) = G \circ \theta$.

Définition 1.1.4 *Soit $\theta(T) \in Hom_A(F,G)$. Si $\theta(T)$ est réversible dans $A[[T]]$, alors on dit que $\theta(T)$ est un isomorphisme de F dans G et on note $G = F^{\theta} = \theta \circ F \circ \theta^{-1}$ avec $\theta \in Iso_A(F,G)$.*

Remarque : Lorsque $F = G$, alors pour $\theta \in \mathrm{Hom}_A(F,F)$ on écrit $\theta \in \mathrm{End}_A(F)$, groupe des endomorphismes de F.

Définition 1.1.5 *Soit $F(X,Y)$ un groupe formel sur A. Il est facile de voir qu'il existe une unique série $\lambda_F(T) \in K[[T]]$ telle que :*

1) $\lambda_F(T) \equiv T \pmod{\deg 2}$,

2) $G_a = F^{\lambda_F}$.

On appelle cette série le "logarithme" du groupe formel F.

Lemme 1.1.1 (Algorithme de Lubin-Tate) [26]

Soient $f(T)$ et $g(T) \in \mathcal{F}_\pi$ et soit $L(X_1,X_2,...,X_n) = \sum_{i=1}^{n} a_i X_i$ une forme linéaire à coefficients dans A. Il existe une unique série $F(X_1,...,X_n)$ à coefficients dans A telle que :

$$\begin{cases} F(X_1,...,X_n) & \equiv & L(X_1,...,X_n) \pmod{\deg 2}, \\ f(F(X_1,...,X_n)) & = & F(g(X_1),...,g(X_n)). \end{cases}$$

Preuve : Posons $X = (X_1, ..., X_n)$ et $g(X) = (g(X_1), ..., g(X_n))$. Par récurrence sur r, on montre que les congruences

$$\begin{cases} F_r(X) & \equiv & L(X) \pmod{\deg 2}, \\ f(F_r(X)) & \equiv & F_r(g(X)) \pmod{\deg(r+1)} \end{cases}$$

ont une solution $F_r(X) \in A[X]$ qui est unique $\pmod{\deg(r+1)}$:
Pour $r = 1$, le système admet $F_1(X) = L(X)$ pour solution. Supposons maintenant que les congruences sont vérifiées pour $r \geq 1$. Alors la solution F_{r+1} doit être cherchée sous la forme $F_{r+1} = F_r + \Delta_r$ avec $\Delta_r \equiv 0 \pmod{\deg(r+1)}$.
Le système

$$\begin{cases} f(F_{r+1}(X)) & \equiv & f(F_r(X)) + \pi\Delta_r(X) \pmod{\deg(r+2)} \\ F_{r+1}(g(X)) & \equiv & F_r(g(X)) + \pi^{r+1}\Delta_r(X) \pmod{\deg(r+2)} \end{cases}$$

nous montre qu' il suffit de prendre

$$\Delta_r(X) \equiv \frac{f(F_r(X)) - F_r(g(X))}{\pi^{r+1} - \pi} \pmod{\deg(r+2)}.$$

Notons que les coefficients de Δ_r sont dans A car

$$f(F_r(X)) - F_r(g(X)) \equiv (F_r(X))^q - F_r(X^q) \equiv 0 \pmod{\pi}.$$

La solution $F(X) = \lim_{r \to +\infty} F_r(X) \in A[[X]]$ est alors l'unique solution du système initial.

Proposition 1.1.1 *Soit $f(T) \in \mathcal{F}_\pi$. Alors il existe un unique groupe formel $F_f(X, Y)$ sur A tel que $f(T) \in End_A(F_f)$.*

Preuve : C'est une application directe du lemme 1.1.1 avec $L(X, Y) = X + Y$ et $f(T) = g(T)$.

Définition 1.1.6 *On appelle groupe formel de Lubin-Tate sur A tout groupe formel construit par la proposition précédente.*

Proposition 1.1.2 *Soient $f(T)$ et $g(T) \in \mathcal{F}_\pi$. Alors pour tout $a \in A$, il existe une unique série notée $[a]_{fg}(T) \in Hom_A(F_g, F_f)$ telle que $[a]_{fg}(T) \equiv aT \pmod{\deg 2}$.*

Preuve : C'est une application du lemme 1.1.1 avec $L(X) = aX$.
Les homomorphismes et endomorphismes de groupes formels de Lubin-Tate vérifient les propriétés suivantes :

Proposition 1.1.3 [26] *Soient $f(T)$, $g(T)$ et $h(T) \in \mathcal{F}_\pi$, et soient a, $b \in A$. Alors :*

1) $[a]_{fg} \circ g(T) = f \circ [a]_{fg}(T)$,

2) $[ab]_{fh}(T) = [a]_{fg} \circ [b]_{gh}(T)$,

3) $[a + b]_{fg}(T) = F_f([a]_{fg}(T), [b]_{fg}(T))$,

4) $[a]_{fg} \circ [b]_{gg}(T) = [b]_{ff} \circ [a]_{fg}(T)$,

5) $[a]_{fg}(T)$ *est réversible si et seulement si* a *est inversible dans* A *et dans ce cas* $[a]_{fg}^{-1}(T) = [a^{-1}]_{gf}(T)$.

Notation : On note $\widetilde{[a]}_{fg}(T)$ la série obtenue en projetant les coefficients de $[a]_{fg}(T)$ sur le corps résiduel $A/\pi A$.

1.1.2 Extensions définies par les groupes formels

Il existe un moyen de construire des extensions abéliennes de corps locaux à l'aide des groupes formels de Lubin-Tate. Le principe consiste à adjoindre des points de torsion au corps de base par le procédé qui est décrit ci-dessous.
On reprend les notations K, A, π et $\mathcal{F}_\pi$ du paragraphe 1.1.1. On note $\overline{K}$ une clôture algébrique de K, puis U le groupe des unités de A et k le corps résiduel $A/\pi A$. Soit $f(T) \in \mathcal{F}_\pi$. Pour tout entier $n \geq 1$ on représente par $f^n(T) = \underbrace{f \circ f \circ ... \circ f(T)}_{n \text{ fois}}$ la composée $n^{\text{ième}}$ de $f(T)$. On note alors

$$\Lambda_n^f = \left\{\lambda \in \overline{K}; f^n(\lambda) = 0; v_\pi(\lambda) > 0\right\}$$

et on pose

$$\Lambda_\infty^f = \bigcup_{n \geq 1} \Lambda_n^f.$$

Soit L une extension algébrique de K d'idéal maximal $M(L)$. La série $f(T)$ permet de définir une structure d' A-module sur $M(L)$ de la manière suivante :
Notons tout d'abord que pour toute série $G(X_1, X_2, ..., X_k) \in A[[X_1, X_2, ..., X_k]]$ et tout vecteur $(x_1, x_2, ..., x_k)$ de $M(L)^k$, l'élément $G(x_1, x_2, ..., x_k)$ est convergent dans $M(L)$ si la série formelle G est sans terme constant. Ceci nous assure que l'on peut définir une addition et une multiplication sur $M(L)$ en posant pour x, $y \in M(L)$ et $a \in A$:

$$\begin{aligned} x + y &= F_f(x, y) \\ ax &= [a]_{ff}(x). \end{aligned}$$

On notera le module ainsi construit $M_f(L)$.
Si $L_1 \subset L$, il est clair que $M_f(L_1)$ est un sous A-module de $M_f(L)$. Si L/L_1 est galoisienne de groupe de Galois G, tout élément τ de G induit un automorphisme du A-module $M_f(L)$; cela provient du fait que τ agit continûment sur L, et que les opérations dans L sont définies par des séries convergentes à coefficients dans K et invariantes sous l'action de τ. Pour f et $g \in \mathcal{F}_\pi$, L'application $x \mapsto [1]_{fg}(x)$ est un A-isomorphisme de $M_g(L)$ dans $M_f(L)$, et cet isomorphisme commute avec les inclusions $L_1 \subset L$ et avec l'action de G.

Restreignons nous maintenant au cas des sous-corps L d'une clôture séparable K_s de K. Pour chaque $f \in \mathcal{F}_\pi$, on peut voir Λ_n^f en tant que sous-module de $M(K_s)$. Pour

f et g dans $\mathcal{F}_\pi$, nous avons $\lambda \in \Lambda_n^f$ si et seulement si $[1]_{gf}(\lambda) \in \Lambda_n^g$. Ainsi l'extension $K(\Lambda_n^f)/K$ dépend seulement de π, et pas de $f \in \mathcal{F}_\pi$; on peut alors la noter $L_{\pi,n}/K$ et son groupe de Galois $G_{\pi,n}$. On pose enfin $L_\pi = K(\Lambda_\infty^f)$, et $G_\pi = \varprojlim G_{\pi,n}$. On a le théorème suivant :

Théorème 1.1.1 (Lubin-Tate [26])
Soit π une uniformisante de A et $f \in \mathcal{F}_\pi$. Alors :

(a) *L'extension $K(\Lambda_\infty^f)/K$ est maximale abélienne totalement ramifiée;*

(b) *Pour tout n, le A-module Λ_n^f est isomorphe à $A/\pi A$;*

(c) *Le A-module Λ_∞^f est isomorphe à K/A;*

(d) *Pour tout $\tau \in G_\pi$, il existe une unique unité u de A telle que $\tau\lambda = [u]_{ff}(\lambda)$ pour $\lambda \in \Lambda_\infty^f$;*

(e) *L'application $\tau \mapsto u$ est un isomorphisme de G_π sur le groupe U des unités de A défini par*

$$[u^{-1}]_{ff} \mapsto u$$

et induisant pour tout n un isomorphisme de $G_{\pi,n}$ sur le quotient $U/(1+\pi^n A)$ de U.

1.2 Corps de normes de Fontaine-Wintenberger des extensions A.P.F.

1.2.1 Définitions

Soit K un corps local et G un sous-groupe fermé du groupe $\mathrm{Aut}(K)$ des automorphismes continus de K. Si π désigne une uniformisante de K, on définit la fonction d'ordre $i_K : G \to \mathbb{N} \cup \{-1\} \cup \{+\infty\}$ par $i_K(\sigma) = v_K(\sigma(\pi)/\pi - 1)$ où v_K désigne la valuation de K définie par π.
Pour tout réel $x \geq 1$, on pose

$$G[x] = \{\sigma \in G, i_K(\sigma) \geq x\},$$

$$G[x]_+ = \{\sigma \in G, i_K(\sigma) > x\}$$

Les $G[x]$ définissent ce que l'on appelle la filtration de ramification du groupe G en numérotation inférieure.
On suppose que les $G[x]$ pour $x \geq -1$ sont d'indice fini dans G. On peut alors définir la fonction ϕ_G de Herbrand [35] par

$$\begin{aligned} \phi_G(x) &= \int_0^x \frac{dt}{(G[0] : G[t])} \text{ si } x \geq 0 \\ &= x \text{ si } -1 \leq x \leq 0 \end{aligned}$$

La fonction ϕ_G est continue et strictement croissante. On dit que G est A.P.F. (arithmétiquement profini) si l'on a

$$\lim_{x \to +\infty} \phi_G(x) = +\infty.$$

C'est en particulier le cas pour $G = \mathrm{Aut}(K)$ avec K de corps résiduel fini.
Lorsque G est A.P.F., la fonction ϕ_G est un homéomorphisme croissant de la demi-droite $[-1, +\infty[$ sur elle-même. On définit alors la fonction ψ_G de Herbrand [35] comme étant la fonction réciproque de ϕ_G et la filtration de ramification en numérotation supérieure de G en posant

$$G(x) = G[\psi_G(x)].$$

On a

$$\begin{aligned} \psi_G(x) &= \int_0^x (G(0) : G(t))dt \text{ si } x \geq 0 \\ &= x \text{ si } -1 \leq x \leq 0 \end{aligned}$$

Lorsque G est fini, $G(x)$ est d'habitude noté G^x et $G[x]$ est noté G_x.

Proposition 1.2.1 (Wintenberger [35])
Soit K un corps local et soit G un groupe A.P.F. d'automorphismes de K. Soit H un sous-groupe fini et distingué de G. Soit K' le corps des points fixes de K sous l'action de H. Alors G/H, considéré comme sous-groupe de $Aut(K')$ est A.P.F. et on a

$$\begin{aligned} \phi_G &= \phi_{G/H} \circ \phi_H \\ \psi_G &= \psi_H \circ \psi_{G/H}. \end{aligned}$$

Soit L une extension galoisienne de K non nécessairement finie de groupe de Galois G. Le groupe G est la limite projective des groupes de Galois $G(K'/K)$, pour K' parcourant l'ensemble des extensions galoisiennes finies de K contenues dans L. Les groupes $Gal(K'/K)(x)$ sont bien définis et cette filtration est compatible avec le système projectif (voir [35]).

On peut donc définir sur G la filtration de ramification en numérotation supérieure en posant pour tout réel $x \geq -1$:

$$G(x) = \lim_{\leftarrow} Gal(K'/K)(x).$$

Il est clair que les $G(x)$ sont des sous-groupes fermés et distingués de G et que pour $x \geq y \geq -1$, on a $G(x) \subset G(y)$.

Définition 1.2.1 *On dit que l'extension L/K est A.P.F. si pour tout $x \geq -1$, le groupe $G(x)$ est ouvert dans G.*

Remarque : Les $G(x)$ étant fermés dans G, l'extension L/K est A.P.F. si et seulement si les $G(x)$ sont d'indice fini dans G.

Définition 1.2.2 *On appelle nombre supérieur de ramification de l'extension L/K, tout réel $x > 0$ tel que $G(x + \epsilon) \neq G(x)$ pour tout $\epsilon > 0$.*

Il est montré dans [35] que l'ensemble de ces nombres est dénombrable.
Les nombres supérieurs de ramification du groupe G sont notés $(b_n(G))_{n\geq 0}$.

Définition 1.2.3 *On appelle nombres inférieurs de ramification les nombres $i_n(G)$ définis par*

$$i_n(G) = \psi_G(b_n(G)).$$

Pour tout entier $i \geq -1$, on pose $K[i] = K^{G[i]}$. Si l'on note $(i_n)_n$ la suite $(i_n(G))_n$, il est clair que l'on a :

$$\begin{aligned} &K = K[-1] \subset K[0], \\ &K[1] = ... = K[i_0], \\ &..... \\ &K[i_{n-1}+1] = ... = K[i_n] \end{aligned}$$

Le corps $K[0]$ (resp. K[1]) est la plus grande extension non (resp. modérément) ramifiée de K contenue dans L.
On a $Gal(K[i]/K[i-1])[i-1] = Gal(K[i]/K[i-1])$ et $\bigcup_{i\in\mathbb{N}} K[i] = L$.

Définition 1.2.4 *La suite $(K[i])_{i\geq -1}$ est appelée la tour des sous-extensions élémentaires de l'extension L/K.*

1.2.2 Construction du corps $X_K(L)$

Pour plus de détails, on pourra consulter [35] et [36].
Pour tout réel x, on désigne par $\{x\}$ (resp. $[x]$) le plus petit entier supérieur ou égal à x (resp. la partie entière de x, c'est-à-dire le plus grand entier inférieur ou égal à x).
D'autre part, pour toute extension M finie d'un corps N, on désigne par $N_{M/N}$ la norme relativement à M et N.
On a :

Lemme 1.2.1 (Wintenberger [35])
Soit N un corps local et soit M une extension galoisienne de N, de groupe de Galois G, telle qu'il existe un entier $i > 0$, avec $G[i] = G$, $G[i]_+ = \{id\}$. Posons $r = \left\{\frac{(p-1)i}{p}\right\}$.
Alors

1) *Pour tous $a, b \in A_M$, on a $N_{M/N}(a+b) \equiv N_{M/N}(a) + N_{M/N}(b) \pmod{P_N^r}$,*

2) *Pour tout $\alpha \in A_N$, il existe $a \in A_M$ tel que $N_{M/N}(a) \equiv \alpha \pmod{P_N^r}$.*

Définition de l'anneau $A_K(L)$:

Soit K un corps local et soit L une extension infinie galoisienne et A.P.F. de K de groupe de Galois G. Soit $(K[i])_{i\geq -1}$ la tour des sous-extensions élémentaires de l'extension L/K. Posons pour tout $i \geq 1$: $r_i = \left\{\frac{(p-1)i}{p}\right\}$, puis

$$\begin{cases} A_{K[i]} = A[i], P_{K[i]} = P[i] \\ N_{K[i+1]/K[i]} = N_i, \overline{A[i]} = A[i]/P[i]^{r_i}. \end{cases}$$

Il résulte facilement du lemme précédent que la composée de la norme $N_i : A[i+1] \to A[i]$, avec la projection canonique $A[i] \to \overline{A[i]}$, est un homomorphisme d'anneaux, qui est surjectif et dont le noyau contient $P[i]^{r_i+1}$; il définit donc, par passage au quotient, un homomorphisme surjectif

$$\overline{N_i} : \overline{A[i+1]} \to \overline{A[i]}.$$

Définition 1.2.5 *On définit l'anneau $A_K(L)$ comme étant la limite projective des $\overline{A[i]}$, pour $i \in \mathbb{N}^*$, les flèches de transition étant les $\overline{N_i} : \overline{A[i+1]} \to \overline{A[i]}$.*

Remarque : Soit $(r'_i)_{i\geq 1}$ une suite d'entiers vérifiant les trois propriétés suivantes :

a) elle est croissante,

b) pour tout $i \geq 1$, on a : $r'_i \leq r_i = \left\{ \dfrac{(p-1)i}{p} \right\}$,

c) on a $\lim\limits_{i\to+\infty} r'_i = +\infty$.

Il est facile de voir [35] que l'on peut définir de manière analogue un anneau $A'_K(L)$ à partir de la suite $(r'_i)_{i\geq 1}$. De plus on vérifie sans peine que les anneaux $A_K(L)$ et $A'_K(L)$ sont canoniquement isomorphes.

Structure de l'anneau $A_K(L)$

Soit a un élément non nul de $A_K(L)$. Si a provient d'une suite $(a_i)_{i\geq 1}$, avec $a_i \in A[i]$, la suite $(v_{K[i]}(a_i))$ est stationnaire et sa limite ne dépend pas du choix des a_i. Posons alors :

$$\begin{aligned} v(a) &= \lim_{i\to+\infty} v_{K[i]}(a_i) \text{ pour } a \neq 0 \\ v(0) &= +\infty. \end{aligned}$$

Puisque l'extension $L/K[0]$ est totalement ramifiée, on peut identifier le corps résiduel k_L de L et les corps résiduels $k_{K[i]}$ des corps $K[i]$, pour $i \geq 0$. Soit α un élément de $k_{K[1]}$. Notons $\alpha_1 = f_{K[1]}(\alpha)$ le représentant multiplicatif de α dans $K[1]$.

Pour tout $i \geq 1$, le degré de l'extension $K[i]/K[1]$ est une puissance de p. Puisque $k_{K[1]}$ est parfait, il en résulte qu'il existe un élément α_i et un seul de $k_{K[1]}$ tel que :

$$\alpha_i^{[K[i]:K[1]]} = \alpha_1.$$

Il est clair que, pour tout $i \geq 1$:

$$N_i(\alpha_{i+1}) = \alpha_i.$$

Il en résulte que la suite $(\alpha_i)_{i\geq 1}$ définit un élément de $A_K(L)$; on le note $f_{L/K}(\alpha)$.

Proposition 1.2.2 (Wintenberger [35])
Soit K un corps local et soit L une extension galoisienne infinie et A.P.F. de K. Alors l'application v munit $A_K(L)$ d'une structure d'anneau de valuation discrète pour laquelle il est complet. On a :

$$v(A_K(L)) = \mathbb{N} \cup \{+\infty\}.$$

La caractéristique de $A_K(L)$ est p. L'application $f_{L/K}$ est un isomorphisme du corps résiduel k_L de L sur le corps résiduel de $A_k(L)$.

Définition 1.2.6 [35] *On définit le corps $X_K(L)$ comme étant le corps des fractions de l'anneau $A_K(L)$. Le corps $X_K(L)$ s'appelle le corps de normes de l'extension A.P.F. L/K.*

Le corps $X_K(L)$ est un corps local de caractéristique p et pour tout $a \in A_K(L)$, on a $v_{X_K(L)}(a) = v(a)$.

1.3 Généralités sur les automates

Nous aurons besoin, pour les interprétations ultérieures, de la notion d'automate fini. Cette partie a pour but de donner les définitions de base concernant les automates ainsi que leur lien avec le problème de l'algébricité des séries.

1.3.1 Définitions

Soit $\mathcal{A}$ un ensemble d'éléments distincts deux à deux.

Définition 1.3.1 *On appelle mot sur $\mathcal{A}$ la donnée d'une suite finie*

$$u = \alpha_n \alpha_{n-1} ... \alpha_1$$

à valeurs dans $\mathcal{A}$:

Définition 1.3.2 *On appelle longueur du mot u son nombre de caractères. On la note $|u|$. L'ensemble des mots sur $\mathcal{A}$ de longueur n est représenté par $\mathcal{A}^n$.*

Définition 1.3.3 *On note $\mathcal{A}^* = \bigcup_{n \geq 0} \mathcal{A}^n$ l'ensemble des mots de longueur finie sur $\mathcal{A}$. On définit sur $\mathcal{A}^*$ l'opération de concaténation de la manière suivante :*
Soient m_1, $m_2 \in \mathcal{A}^*$. Si l'on pose $m_1 = \alpha_r \alpha_{r-1} ... \alpha_1$ et $m_2 = \alpha'_s \alpha'_{s-1} ... \alpha'_1$, alors le mot $m_1 m_2$ est le mot $\alpha_r \alpha_{r-1} ... \alpha_1 \alpha'_s \alpha'_{s-1} ... \alpha'_1 \in \mathcal{A}^*$.

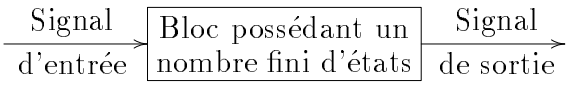
Définition 1.3.4 *On appelle langage sur $\mathcal{A}$ tout sous-ensemble $\mathcal{L}$ de $\mathcal{A}^*$.*

Plusieurs opérations peuvent être définies sur les langages :

- Réunion ensembliste : $\mathcal{L}_1 \bigcup \mathcal{L}_2$;
- Intersection : $\mathcal{L}_1 \bigcap \mathcal{L}_2$;
- Produit de concaténation : $\mathcal{L}_1.\mathcal{L}_2 = \{u = m_1 m_2 \text{ avec } m_1 \in \mathcal{L}_1 \text{ et } m_2 \in \mathcal{L}_2\}$. On définit alors $\mathcal{L}^n = \underbrace{\mathcal{L}.\mathcal{L}...\mathcal{L}}_{n \text{ fois}}$;
- Opération $*$: $\mathcal{L}^* = \bigcup_{n=0}^{\infty} \mathcal{L}^n$.

Définition 1.3.5 *Un langage $\mathcal{L}$ est dit régulier s'il est obtenu à partir d'un langage fini par un nombre fini d'opérations $\bigcup$, $\bigcap$, ., $*$.*

Définition 1.3.6 *On appelle "automate" (fini) un "système" recevant un signal d'entrée, émettant un signal de sortie et possédant un nombre fini d'états (voir la modélisation mathématique ci-dessous pour une définition de la notion d'état).*



Modélisation mathématique d'un automate : Il s'agit de la donnée de :

- Q : ensemble fini des états;
- $q_0 \in Q$: état initial;
- Σ : alphabet fini (d'entrée);
- Γ : alphabet fini (de sortie);
- $T : Q \times \Sigma \longrightarrow Q$: fonction de transition;
- $S : Q \longrightarrow \Gamma$: signal de sortie.

Remarque : On peut interpréter l'application $T : Q \times \Sigma \longrightarrow Q$ comme étant un ensemble d'applications T_0, T_1,...,T_{k-1} :

$$\begin{array}{ccc} Q & \longrightarrow & Q \\ q & \mapsto & T_i(q) = T(q, a_i) \end{array}$$

où $\Sigma = \{a_0, a_1, ..., a_{k-1}\}$.
On représente l'automate par $\mathbb{A} = \mathbb{A}(Q, q_0, \Sigma, \Gamma, T, S)$.

Définition 1.3.7 *Si $Card(\Sigma) = k$, on dit que $\mathbb{A}$ est un k-automate.*

Remarque : T se prolonge naturellement de Σ à Σ^* par $T(q, u_1u_2) = T(T(q, u_1), u_2)$. La notion de langage reconnaissable par un automate peut être introduite lorsque l'on définit parmi les états de ce dernier un certain nombres d'états terminaux :

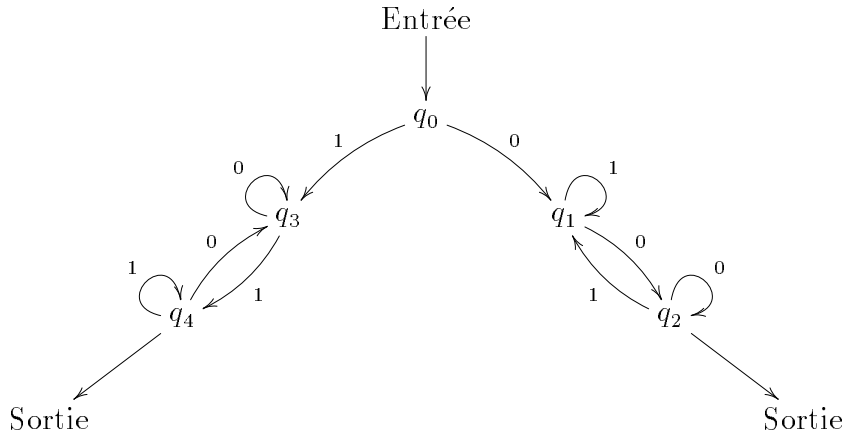
Définition 1.3.8 *Le mot $u = u_n u_{n-1} ... u_1$ est dit reconnaissable si $T(q_0, u)$ est un état terminal.*

Définition 1.3.9 *Soit $\mathcal{F}(\mathbb{A})$ l'ensemble des états terminaux de $\mathbb{A}$. On définit alors le comportement $|\mathbb{A}|$ de l'automate $\mathbb{A}$ par :*

$$|\mathbb{A}| = \{u \in \Sigma^* | T(q_0, u) \in \mathcal{F}(\mathbb{A})\} .$$

Proposition 1.3.1 *Un langage $\mathcal{L}$ est régulier si et seulement s'il existe un automate $\mathbb{A}$ tel que $\mathcal{L} = |\mathbb{A}|$.*

Exemple : Automate reconnaissant les mots binaires commençant et finissant par la même lettre :



Si lors de la lecture du dernier caractère l'automate $\mathbb{A}$ est en l'état q_2 ou q_4, c'est que le mot en entrée appartient à $|\mathbb{A}|$.

1.3.2 L'algébricité des séries d'un point de vue "automatique"

Une particularité des automates (finis) est qu'il permettent "d'engendrer" les coefficients d'une série de $\mathbb{F}_q[[T]]$ lorsque celle-ci est algébrique sur le corps $\mathbb{F}_q(T)$.
Nous rappelons rapidement le résultat principal. Pour plus de précision, on peut consulter les travaux de Christol, Kamae, Mendès France et Rauzy dans [10] ou encore d'Allouche dans [1].

Définition 1.3.10 *Soit γ un nombre entier. On appelle γ-noyau d'une suite $a = (a_n)_{n\geq 0}$ à coefficients dans un alphabet fini l'ensemble*

$$N_\gamma(a) = \{n \mapsto a_{\gamma^k n+r}; k \geq 0; 0 \leq r \leq \gamma^k - 1\}.$$

Définition 1.3.11 *Une suite $(u_n)_{n\in\mathbb{N}}$ est dite engendrée par un γ-automate (ou γ-automatique) si lorsqu'on écrit $n = n_0 + n_1\gamma + n_2\gamma^2 + ... + n_l\gamma^l$ avec $0 \leq n_i \leq \gamma - 1$ pour $0 \leq i \leq l$ on a : $u_n = S(T_{n_l}(T_{n_{l-1}}(...(T_{n_1}(T_{n_0}(q_0)))...)))$.*

Le résultat principal est :

Théorème 1.3.1 (Christol [9]), voir aussi [10] et [12]
Soit $(u_n)_{n\geq 0}$ une suite à coefficients dans $\mathbb{F}_q$. Alors les assertions suivantes sont équivalentes :

(i) *la suite $(u_n)_{n\geq 0}$ est q-automatique,*

(ii) *la série $\sum_{n\geq 0} u_n X^n$ est algébrique sur $\mathbb{F}_q(X)$,*

(iii) *le cardinal de $N_q((u_n)_n)$ est fini.*

Remarque : L'assertion (ii) n'est pas évoquée dans [12].

1.4 Un survol des résultats d'algébricité

Sharif et Woodcock [32] ainsi qu'Harase [19] obtiennent la généralisation suivante du théorème 1.3.1, généralisation que l'on trouve, sous la forme qui suit, dans [3].

Théorème 1.4.1 ([3], [32], [19])
Soit K un corps commutatif de caractéristique non nulle p, et soit $\overline{K}$ un corps parfait qui contient K (par exemple une clôture algébrique ou radicielle de K). Soit $(a(n_1, ..., n_r))$ une suite à valeurs dans K, soit enfin $s \geq 1$ un entier et $q = p^s$. Les quatre propriétés suivantes sont équivalentes :

(i) *La série formelle $\sum_{n_i\geq 0} a(n_1, ..., n_r)X_1^{n_1}...X_r^{n_r}$ est algébrique sur $K(X_1, ..., X_r)$,*

(ii) *Il existe un $\overline{K}$-espace vectoriel $\mathcal{W}$ de suites, de dimension finie sur $\overline{K}$, qui contient la suite a et qui est stable par les applications*

$$(b(n_1, ..., n_r)) \mapsto (b^{1/q}(qn_1 + j_1, ..., qn_r + j_r)),$$

pour $0 \leq j_1, ..., j_r \leq q - 1$,

(iii) *L'espace vectoriel engendré sur $\overline{K}$ par l'ensemble des suites*

$$\{(a^{1/q^k}(q^k n_1 + j_1, ..., q^k n_r + j_r)); k \geq 0; 0 \leq j_1, ..., j_r \leq q - 1\}$$

est de dimension finie sur K,

(iv) *Il existe un entier $c \geq 1$, une famille de matrices carrées à c lignes et c colonnes $\{A_{j_1,...,j_r}; 0 \leq j_1, ..., j_r \leq q - 1\}$, et une suite $(U(n_1, ...n_r))$ à valeurs dans $\overline{K}^c$ tels que :*

- *Si ϕ est la première projection canonique de $\overline{K}^c$ sur $\overline{K}$, on a $\phi(U) = a$,*
- $\forall (j_1, ..., j_r) \in [0, q-1]^r, \forall (n_1, ..., n_r) \in \mathbb{N}^r$, *on a :*

$$U^{1/q}(q_1^n + j_1, ..., q_r^n + j_r)) = A_{j_1,...,j_r} U(n_1, ..., n_r)$$

où $U^{1/q}$ est le vecteur dont les composantes dans la base canonique sont des racines $q^{ièmes}$ de celles de U.

Définition 1.4.1 *Soit λ un entier p-adique. On définit l'élévation de $(1+T)$ à la puissance λ par*

$$(1+T)^\lambda = \sum_{n=0}^{+\infty} \left(\begin{array}{c} \lambda \\ n \end{array} \right) T^n \in \mathbb{Z}_p[[T]]$$

où $\left(\begin{array}{c} \lambda \\ n \end{array} \right) = \dfrac{\lambda(\lambda-1)...(\lambda-n+1)}{n!} \in \mathbb{Z}_p$.

Nous avons le théorème ci-dessous dû entre autres à Robba dans [29] mais aussi à Mendès France et van der Poorten dans [28], généralisé par Allouche, Mendès France et van der Poorten dans [5] :

Théorème 1.4.2 ([29], [28], [5])
Soit $\lambda \in \mathbb{Z}_p$. Les assertions suivantes sont équivalentes :

(i) $\lambda \in \mathbb{Q}$,

(ii) *La série $(1+T)^\lambda \bmod p$ est algébrique sur $\mathbb{F}_p(T)$.*

On obtient dans [5] la généralisation suivante :

Théorème 1.4.3 (Allouche, Mendès France, van der Poorten, [5])
Soient λ_1, λ_2,...,λ_n des entiers p-adiques. Nous avons les équivalences :

(i) *Les entiers p-adiques 1, λ_1, λ_2,..., λ_n sont $\mathbb{Z}$-linéairement indépendants,*

(ii) *Les séries formelles $(1+T)^{\lambda_1}$, $(1+T)^{\lambda_2}$,..., $(1+T)^{\lambda_n}$ réduites modulo p sont algébriquement indépendantes sur $\mathbb{F}_p(T)$.*

Définition 1.4.2 *Soit K un corps et soient $u = (u_n)_n$ et $v = (v_n)_n$ deux suites à coefficients dans K. On définit le produit de Hadamard $w = u * v$ des suites u et v par*

$$w_n = u_n v_n \text{ pour } n \in \mathbb{N}.$$

De même, on définit le produit de Hadamard des séries $U = \sum_{n=0}^{+\infty} u_n T^n$ et $V = \sum_{n=0}^{+\infty} v_n T^n$ par

$$U * V = \sum_{n=0}^{+\infty} u_n v_n T^n.$$

Théorème 1.4.4 (Deligne [14], voir aussi [15] et [3])
Soient deux séries formelles à coefficients dans un corps de caractéristique strictement positive, et à un nombre fini de variables X_1,...,X_m. Si ces deux séries sont algébriques sur $K(X_1, ..., X_m)$, alors il en est de même de leur produit de Hadamard.

1.5 Résultats préliminaires sur les séries

1.5.1 Définition

Soient K un corps commutatif et T une variable formelle sur K.

Définition 1.5.1 *On dit qu'une série $\alpha(T) \in K[[T]]$ est algébrique sur $K(T)$ s'il existe $P(X) \in K(T)[X]$ non trivial tel que $P(\alpha(T)) = 0$.*

1.5.2 Propriétés d'algébricité

Proposition 1.5.1 *Soit une série $\alpha(T) \in K[[T]]$. On suppose que $\alpha(T)$ est réversible. Les assertions suivantes sont équivalentes :*

(i) *La série $\alpha(T)$ est algébrique sur $K(T)$,*

(ii) *La série $\alpha^{-1}(T)$ est algébrique sur $K(T)$.*

Preuve : Supposons que $\alpha(T)$ soit algébrique sur $K(T)$. Cela signifie que $\alpha(T)$ est racine d'un polynôme non nul à coefficients dans $K(T)$. En d'autres termes, il existe $f(X,Y) \in K[X,Y]\backslash K$ tel que

$$f(\alpha(T), T) = 0 \text{ avec } \deg_X f(X,Y) \geq 1.$$

Or, $(\alpha(T), T)$ peut s'écrire

$$(\alpha(T), T) = (\theta, \alpha^{-1}(\theta)).$$

Ainsi, le point $(\theta, \alpha^{-1}(\theta))$ est sur la courbe $f(X,Y) = 0$. De plus, il est clair que $\theta(= \alpha)$ est une variable formelle sur K car c'est une série en T d'ordre 1. En particulier, $\alpha(T)$ est transcentante sur K. Pour conclure que $\alpha^{-1}(T)$ est algébrique sur $K(T)$, on remarque que c'est équivalent à montrer que $\alpha^{-1}(\theta)$ est algébrique sur $K(\theta)$. Cela revient à s'assurer que $\deg_Y f(X,Y) \geq 1$. Or, si l'on avait le contraire, le polynôme $f(X,Y)$ appartiendrait à $K[X]\backslash K$ et dans ce cas, $\alpha(T)$ serait algébrique sur K, ce qui est impossible.
Par symétrie, on obtient l'équivalence.

Lemme 1.5.1 *Soient $\alpha(T)$ et $\beta(T)$ deux séries de $K[[T]]$. On suppose que la série $\alpha(T)$ est algébrique sur $K(T)$ avec $Ord_T(\alpha) \geq 1$ et que la série $\beta(T)$ est réversible. Alors si la série $(\alpha \circ \beta)(T)$ est algébrique sur $K(T)$, la série $\beta(T)$ est algébrique sur $K(T)$.*

Preuve : La série $\beta(T)$ étant réversible, elle est d'ordre 1 en T et "définit" ainsi une variable formelle sur K.
L'algébricité de $\alpha \circ \beta(T)$ sur $K(T)$ implique l'existence d'un polynôme $f(X,Y) \in K[X,Y]\backslash K$ tel que

$$f(\alpha \circ \beta, T) = 0 \text{ avec } \deg_X f(X,Y) \geq 1.$$

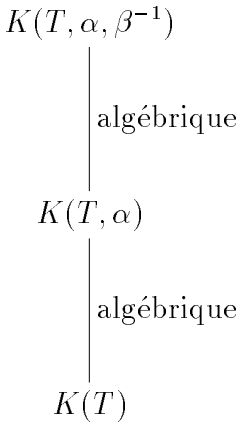
Or, le point $(\alpha \circ \beta, T)$ peut s'écrire

$$(\alpha(\theta), \beta^{-1}(\theta))$$

avec $\theta = \beta$. Montrons que $\deg_Y f(X,Y) \geq 1$. En effet, si ce n'était pas le cas, cela voudrait dire que $\alpha(\theta)$ est algébrique sur K, ce qui est impossible puisque $Ord_\theta(\alpha(\theta)) \geq 1$.
Ainsi, $\beta^{-1}(\theta)$ est algébrique sur $K(\alpha(\theta))$, que l'on peut écrire

$$\text{“}\beta^{-1}(T) \text{ est algébrique sur } K(\alpha(T))\text{”}.$$

La série $\beta^{-1}(T)$ est donc algébrique sur $K(T, \alpha(T))$. Comme $\alpha(T)$ est algébrique sur $K(T)$, on obtient que $\beta^{-1}(T)$ est algébrique sur $K(T)$.



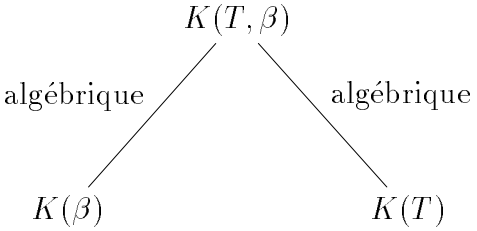
On conclut à l'algébricité de $\beta(T)$ sur $K(T)$ en utilisant la prosposition précédente.

Lemme 1.5.2 *Soient $\alpha(T) \in K[[T]]$ et $\beta(T) \in TK[[T]]$ ($\beta \neq 0$). Supposons que les séries $(\alpha \circ \beta)(T)$ et $\beta(T)$ sont algébriques sur $K(T)$. Alors la série $\alpha(T)$ est algébrique sur $K(T)$.*

Preuve : Remarquons que $\beta(T)$ étant une série d'ordre supérieur ou égal à 1, elle se comporte comme une variable formelle sur K. De plus, elle est algébrique sur $K(T)$. Donc il existe un polynôme $f(X,Y) \in K[X,Y] \backslash K$ tel que

$$f(\beta, T) = 0 \text{ et } \deg_X f(X,Y) \geq 1.$$

Montrons que T est algébrique sur $K(\beta)$:
On a $\deg_Y f(X,Y) \geq 1$ car sinon cela signifierait que $\beta(T)$ est algébrique sur K. On en déduit bien l'algébricité de T sur $K(\beta)$. Ainsi, l'extension $K(T,\beta)/K(\beta)$ est algébrique.



De plus, la série $\alpha \circ \beta(T)$ étant algébrique sur $K(T)$, elle l'est a fortiori sur $K(T, \beta)$. Il vient alors que $\alpha \circ \beta$ est algébrique sur $K(\beta)$, que l'on peut écrire "$\alpha(\beta)$ est algébrique sur $K(\beta)$" ou encore

"$\alpha(T)$ est algébrique sur $K(T)$".

Remarque : Un autre moyen de voir les choses est de raisonner à l'aide des degrés de transcendance :
Soit $\beta = \beta(T) \in K[[T]]$. Le degré de transcendance de $K(T, \beta)/K$ est 1 ou 2; si β est algébrique sur $K(T)$, c'est 1 et le degré de transcendance de $K(T, \beta)/K(\beta)$ est 0 ou 1. Si c'est 1 alors le degré de transcendance de $K(\beta)/K$ est 0, c'est-à-dire β est algébrique sur K (ce qui ne peut se produire que si $\beta(T)$ est réduit à son terme constant). Le degré de transcendance de $K(T, \beta)/K(\beta)$ est donc 0 et T est algébrique sur $K(\beta)$.

Maintenant si $\alpha \circ \beta(T)$ est algébrique sur $K(T)$, le degré de transcendance de $K(T, \beta, \alpha \circ \beta)/K(T, \beta)$ est 0, donc le degré de transcendance de $K(T, \beta, \alpha \circ \beta)/K(\beta)$ est 0. Autrement dit, $\alpha \circ \beta$ est algébrique sur $K(\beta)$ et par transport de structure $(\beta \mapsto T)$, $\alpha(T)$ est algébrique sur $K(T)$.

Lemme 1.5.3 *Soient $\alpha(T)$ et $\beta(T)$ deux séries de $K[[T]]$ algébriques sur $K(T)$. On suppose que $\beta(T) \in TK[[T]]$ et est non nulle. Alors la composée $(\alpha \circ \beta)(T)$ est une série algébrique sur $K(T)$.*

Preuve : Il est clair que $\beta = \beta(T)$ est un élément transcendant sur K et qu'il peut être interprété comme étant une variable formelle sur K (car $Ord_T(\beta) \geq 1$). L'algébricité de $\alpha(T)$ sur $K(T)$ peut alors s'écrire :

"$\alpha(\beta)$ est algébrique sur $K(\beta)$."

La série $\beta(T)$ étant algébrique sur $K(T)$, l'extension $K(\beta, T)/K(T)$ est algébrique. Or, $\alpha \circ \beta$ est algébrique sur $K(\beta)$ donc sur $K(\beta, T)$ et, par transitivité, sur $K(T)$.

$$
\begin{array}{c}
K(T, \beta, \alpha \circ \beta) \\
\Big| \\
\text{algébrique} \\
\Big| \\
K(T, \beta) \\
\Big| \\
\text{algébrique} \\
\Big| \\
K(T)
\end{array}
$$

Proposition 1.5.2 *Soient $\alpha(T)$, $\beta(T)$ et $\gamma(T)$ trois séries de $K[[T]]$ telles que*

$$\alpha \circ \beta(T) = \beta \circ \gamma(T).$$

On suppose que $\beta(T)$ est algébrique sur $K(T)$, appartient à $TK[[T]]$ et est non nulle. Alors si α et γ sont réversibles, les assertions suivantes sont équivalentes :

(i) *$\alpha(T)$ est algébrique sur $K(T)$,*

(ii) *$\gamma(T)$ est algébrique sur $K(T)$.*

Preuve : Supposons $\alpha(T)$ algébrique. Par le lemme 1.5.3, $\alpha \circ \beta(T)$ est algébrique. On en déduit que $\beta \circ \gamma(T)$ est algébrique. Le lemme 1.5.1 implique alors que $\gamma(T)$ est algébrique.
Supposons maintenant que $\gamma(T)$ est algébrique. Par le lemme 1.5.3, $\beta \circ \gamma(T)$ est algébrique. On en déduit que $\alpha \circ \beta(T)$ est algébrique. Le lemme 1.5.2 permet de conclure à l'algébricité de $\alpha(T)$.

Proposition 1.5.3 *Soient $\alpha(T)$ et $\beta(T)$ deux séries réversibles de $K[[T]]$. On a les résultats suivants :*

(i) *Si les séries $\alpha(T)$ et $\beta(T)$ sont algébriques sur $K(T)$, la composée $\alpha \circ \beta(T)$ l'est aussi,*

(ii) *Si $\alpha(T)$ est algébrique et $\beta(T)$ transcendante, la composée $\alpha \circ \beta(T)$ est transcendante,*

(iii) *Si $\alpha(T)$ est transcendante et $\beta(T)$ algebrique, la composée $\alpha \circ \beta(T)$ est transcendante.*

Preuve :

(i) Cette assertion est établie par le lemme 1.5.3.

(ii) Cette assertion est la contraposée du lemme 1.5.1.

(iii) Il s'agit de la contraposéee du lemme 1.5.2.

Chapitre 2

Automorphismes de corps locaux et p-automates

2.1 Algorithme de Lubin-Tate et p-automates

2.1.1 Le groupe multiplicatif sur $\mathbb{Z}_p$

On pose $A = \mathbb{Z}_p$, $K = \mathbb{Q}_p$ et $\pi = p$. Le groupe des éléments inversibles de $\mathbb{Z}_p$ est noté U_p. Soit $f(T) = (1+T)^p - 1 \in \mathcal{F}_p$. Par la proposition 1.1.1, il existe un unique groupe formel F_f sur $\mathbb{Z}_p$ (de Lubin-Tate) admettant $f(T)$ pour endomorphisme. On a $F_f(X,Y) = X + Y + XY$. On appelle ce groupe formel le groupe multiplicatif.
Les endomorphismes $[a]_{ff}(T)$ ont alors une forme explicite :

$$[a]_{ff}(T) = (1+T)^a - 1 \in \mathbb{Z}_p[[T]]$$

et le théorème 1.4.2 peut s'écrire, en termes d'endomorphismes de groupes formels :

Théorème 2.1.1 *Soit $a \in \mathbb{Z}_p$. Les assertions suivantes sont équivalentes :*

(i) $a \in \mathbb{Q}$,

(ii) *La série $\widetilde{[a]}_{ff}(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Nous allons voir maintenant que s'il existe des groupes formels de Lubin-Tate isomorphes sur $\mathbb{Z}_p$ au groupe multiplicatif par un isomorphisme dont la réduction modulo p est algébrique sur $\mathbb{F}_p(T)$, alors l'équivalence du théorème précédent est également vérifiée pour ces derniers.

2.1.2 Groupes de Lubin-Tate particuliers

Proposition 2.1.1 *Soient $f(T) = (1+T)^p - 1 \in \mathcal{F}_p$, $g(T) \in \mathcal{F}_p$ et soit $F_g(X,Y)$ le groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ admettant $g(T)$ pour endomorphisme. Supposons qu'il existe $u \in U_p \bigcap \mathbb{Q}$ tel que $\widetilde{[u]}_{fg}(T)$ soit algébrique sur $\mathbb{F}_p(T)$. Alors :*

1) *Pour tout* $v \in \mathbb{Z}_p \bigcap \mathbb{Q}$, $\widetilde{[v]}_{fg}(T)$ *et* $\widetilde{[v]}_{gf}(T)$ *sont algébriques sur* $\mathbb{F}_p(T)$,

2) *Soit* $v \in \mathbb{Z}_p$, *alors* $v \in \mathbb{Q}$ *si et seulement si* $\widetilde{[v]}_{gg}(T)$ *est algébrique sur* $\mathbb{F}_p(T)$.

Preuve : 1) Si $u \in U_p \bigcap \mathbb{Q}$ alors par le théorème 2.1.1, la série $\widetilde{[u]}_{ff}(T)$ est algébrique sur $\mathbb{F}_p(T)$. Or on peut écrire que

$$\widetilde{[u]}_{ff}(T) = \widetilde{[u]}_{fg} \circ \widetilde{[1]}_{gf}(T).$$

Donc $\widetilde{[1]}_{gf}(T) = \widetilde{[u^{-1}]}_{gf} \circ \widetilde{[u]}_{ff}(T)$ est algébrique en tant que composée de deux séries algébriques (proposition 1.5.3). Soit $v \in U_p \bigcap \mathbb{Q}$. Alors $\widetilde{[v]}_{ff}(T) = \widetilde{[v]}_{fg} \circ \widetilde{[1]}_{gf}(T)$ est algébrique. On en déduit que $\widetilde{[v]}_{fg}(T)$ est algébrique.
Comme $v^2 \in U_p \bigcap \mathbb{Q}$, la série $\widetilde{[v^2]}_{ff}(T) = \widetilde{[v]}_{fg} \circ \widetilde{[v]}_{gf}(T)$ est algébrique et on obtient alors l'algébricité de $\widetilde{[v]}_{gf}(T)$.
2) On a $v \in \mathbb{Q} \Leftrightarrow \widetilde{[v]}_{ff}(T)$ algébrique. Or $\widetilde{[v]}_{gg}(T) = \widetilde{[1]}_{gf} \circ \widetilde{[v]}_{ff} \circ \widetilde{[1]}_{fg}(T)$ avec $\widetilde{[1]}_{gf}(T)$ et $\widetilde{[1]}_{fg}(T)$ algébriques, d'où la conclusion.

Avant de pouvoir s'assurer qu'il existe effectivement de tels groupes formels, nous aurons besoin d'une proposition qui est une conséquence du Lemme de l'Équation Fonctionnelle. La partie suivante est un énoncé de ce lemme.

2.1.3 L'Équation Fonctionnelle

Nous allons voir dans cette partie une méthode générale de construction de groupes formels décrite avec plus de détails dans [21].

Ingrédients et construction

Soient K un anneau quelconque et A un sous-anneau de K, soient σ un homomorphisme d'anneaux $K \to K$, I_A un idéal de A, p un nombre premier, q une puissance de p et s_1, s_2,... des éléments de K. On suppose que les conditions suivantes sont réalisées :

$$\begin{array}{l} \sigma(A) \subset A, \\ \sigma(a) \equiv a^q \pmod{I_A} \text{ pour tout } a \in A, \\ p \in I_A, \\ s_i I_A = \{s_i b, b \in I_A\} \subset A,\ i = 1, 2, ... \end{array}$$

Remarquons que la congruence $\sigma(a) \equiv a^q \pmod{I_A}$ pour tout $a \in I_A$ implique que $\sigma(A) \subset A$ et que $\sigma(I_A) \subset I_A$. De plus, on suppose que l'on a

$$I_A^r b \subset I_A \Rightarrow I_A^r \sigma(b) \subset I_A$$

pour tout $r \in \mathbb{N}$ et tout $b \in K$. Cette propriété est satisfaite si, par exemple, I_A est principal, $I_A = (c)$, avec $c \in A$ tel que $\sigma(c) = uc$ pour $u \in A$.
C'est le cas en particulier si K est un corps local de corps résiduel k fini de caractéristique p, d'anneau des entiers A, avec $q = p$, I_A idéal maximal de A, $\sigma : K \to K$ le Frobenius de K (c'est-à-dire l'unique endomorphisme de K tel que $\sigma(a) \equiv a^p \pmod{I_A}$ pour tout $a \in A$), et $s_i \in \pi^{-1}A$ où π est une uniformisante de A.

Soit maintenant la série

$$g(X) = \sum_{i=1}^{+\infty} b_i X^i \in A[[X]].$$

Nous construisons la série $f_g(X)$ définie par l'équation fonctionnelle

$$f_g(X) = g(X) + \sum_{i=1}^{+\infty} s_i \sigma^i * f_g(X^{q^i}), \tag{2.1}$$

où $\sigma^i * f_g(X)$ est la série obtenue en appliquant l'endomorphisme σ^i aux coefficients de $f_g(X)$.
La série $f_g(X)$ dépend évidemment de $g(X)$, σ, q, s_1, s_2,...Notons qu'en fait, l'équation 2.1 définit une récurrence sur les coefficients de $f_g(X)$.
Posons $f_g(X) = \sum_{i=1}^{+\infty} d_i X^i$. Les d_n sont alors déterminés de la manière suivante : écrivons $n = q^r m$ avec $(m, q) = 1$. On a :

$$d_n = b_n + s_1 \sigma(d_{n/q}) + ... + s_r \sigma^r(d_{n/q^r}).$$

Remarque : Si q ne divise pas n, on a $d_n = b_n$.

Le Lemme de l'Équation Fonctionnelle

Lemme 2.1.1 [21] *Soient A, K, σ, I_A, p, q, s_1, s_2,... comme dans le paragraphe précédent et soient*

$$g(X) = \sum_{i=1}^{\infty} b_i X^i$$

et

$$\overline{g}(X) = \sum_{i=1}^{\infty} \overline{b}_i X^i$$

deux séries à coefficients dans A. On suppose que b_1 est inversible dans A. Nous avons les résultats suivants :

a) *La série $F_g(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$ est à coefficients dans A,*

b) *La série $f_g^{-1}(f_{\overline{g}}(X))$ est à coefficients dans A,*

c) *Si* $h(X) = \sum_{n=1}^{+\infty} c_n X^n$ *est une série à coefficients dans* A*, alors il existe une série* $\widehat{h}(X) = \sum_{n=1}^{+\infty} \widehat{c}_n X^n$ *avec* $\widehat{c}_n \in A$ *pour* $n = 1, 2, ...$ *telle que* $f_g(h(X)) = f_{\widehat{h}}(X)$,

d) *Si* $\alpha(X) \in A[[X]]$, $\beta(X) \in K[[X]]$ *et si* $r \in \mathbb{N}^*$*, alors on a :*

$$\alpha(X) \equiv \beta(X) \pmod{I_A^r A[[X]]} \Leftrightarrow f_g(\alpha(X)) \equiv f_g(\beta(X)) \pmod{I_A^r A[[X]]}.$$

Preuve : Voir annexe B.

Si $f_g(X)$ et $f_{\overline{g}}(X)$ sont deux séries formelles obtenues par l'équation fonctionnelle 2.1 initialisée avec les mêmes données sauf éventuellement la série $g(X) \neq \overline{g}(X)$, alors nous dirons que $f_g(X)$ et $f_{\overline{g}}(X)$ satisfont le même type d'équation fonctionnelle.
Les parties b) et c) du lemme nous permettent d'affirmer que si $f(X)$ et $\overline{f}(X)$ satisfont l'équation fonctionnelle avec $f(X) \equiv \overline{f}(X) \equiv X \pmod{\deg 2}$, alors les groupes formels $F(X,Y) = f^{-1}(f(X) + f(Y))$ et $\overline{F}(X,Y) = \overline{f^{-1}}(\overline{f}(X) + \overline{f}(Y))$ sont isomorphes sur A si et seulement si $f(X)$ et $\overline{f}(X)$ satisfont une équation fonctionnelle du même type.

Proposition 2.1.2 *Soit* A *l'anneau des entiers d'un corps local* K *de corps résiduel* k *fini de cardinal* q*. On note* π *une uniformisante de* A*.*
Alors les groupes de Lubin-Tate $F_e(X,Y)$ *sur* A *obtenus pour* $e(T) \in \mathcal{F}_\pi$ *sont les groupes formels obtenus par le lemme de l'équation fonctionnelle avec les données* A*,* K*,* q*,* $I_A = (\pi)$*,* $\sigma = id$*,* $s_1 = \pi^{-1}$*,* $s_2 = s_3 = ... = 0$ *et* $g(X) \in A[[X]]$ *vérifiant* $g(X) \equiv X \pmod{\deg 2}$.
La correspondance est donnée par

$$g(X) \mapsto f_g^{-1}(\pi f_g(X)) \in \mathcal{F}_\pi.$$

Preuve : Si l'on applique le lemme de l'équation fonctionnelle 2.1.1 avec les données ci-dessus, on obtient pour solution la série $f(X)$ vérifiant

$$f(X) = X + \frac{1}{\pi} f(X^q). \tag{2.2}$$

Soient

$$F(X,Y) = f^{-1}(f(X) + f(Y))$$

et

$$[\pi]_F(X) = f^{-1}(\pi f(X)).$$

En multipliant 2.2, on fait apparaître que $\pi f(X)$ vérifie l'équation fonctionnelle

$$\pi f(X) = \pi X + \frac{1}{\pi} \pi f(X^q).$$

Ainsi les parties a) et b) du lemme de l'équation fonctionnelle impliquent que $F(X,Y)$ et $[\pi]_F(X)$ sont à coefficients dans A et $F(X,Y)$ devient un groupe formel sur A admettant $[\pi]_F(X)$ pour endomorphisme.

On va maintenant s'assurer que ce groupe formel est de Lubin-Tate.
Montrons que

$$[\pi]_F(X) \equiv X^q \pmod{\pi}. \tag{2.3}$$

On peut facilement voir que cette congruence est vraie modulo degré $q+1$ par définition de $[\pi]_F(X)$. Le résultat s'établit par récurrence :
Supposons la congruence vérifiée modulo degré m avec $m > q$.
Alors, modulo (π, degré $m+1$), nous avons :

$$\begin{aligned} f([\pi]_F(X)) &\equiv [\pi]_F(X) + \pi^{-1} f([\pi]_F(X)^q) \\ &\equiv [\pi]_F(X) + \pi^{-1} f(X^{q^2}), \end{aligned}$$

$$\pi f(X) \equiv \pi X + f(X^q) \equiv \pi X + X^q + \pi^{-1} f(X^{q^2}).$$

Il vient ainsi : $[\pi]_F(X) \equiv X^q \pmod{\pi, \deg m+1}$, d'où la congruence 2.3.
Remarque : On peut également obtenir le résultat en utilisant la partie d) du lemme de l'équation fonctionnelle.

La série $[\pi]_F(X)$ est donc un élément de $\mathcal{F}_\pi$. Par unicité des groupes formels de Lubin-Tate, on en déduit que la série $F(X,Y) = F_e(X,Y)$ est l'unique groupe formel de Lubin-Tate sur A admettant $e(X) = [\pi]_F(X)$ pour endomorphisme.

Soit maintenant $\overline{e}(X) \in \mathcal{F}_\pi$ et $F_{\overline{e}}(X,Y)$ le groupe formel de Lubin-Tate sur A admettant $\overline{e}(X)$ pour endomorphisme. Alors $F_{\overline{e}}(X,Y)$ est isomorphe sur A à $F_e(X,Y)$. Nous avons :

$$F_{\overline{e}}(X,Y) = \overline{f}^{-1}(\overline{f}(X) + \overline{f}(Y))$$

avec

$$\overline{f}(X) = f([1]_{e,\overline{e}}(X)).$$

Par le c) du lemme de l'équation fonctionnelle, la série $\overline{f}(X)$ vérifie une équation fonctionnelle du même type que $f(X)$.
De plus, par la partie b) du lemme, deux séries vérifiant le même type d'équation fonctionnelle donnent deux groupes formels isomorphes sur A. Si $\alpha(X) \in A[[X]]$ avec $\alpha(X) \equiv X \pmod{\deg 2}$, nous avons modulo π :

$$\alpha^{-1}([\pi]_F(\alpha(X))) \equiv \alpha^{-1}(\alpha(X)^q) \equiv \alpha^{-1}(\alpha(X^q)) \equiv X^q$$

et ainsi si $\overline{F}(X,Y)$ est isomorphe sur A à $F(X,Y)$, alors

$$[\pi]_{\overline{F}}(X) \equiv [\pi]_F(X) \equiv X^q \pmod{\pi}.$$

Remarque : La série $g(X)$ étant unitaire, la série $f_g(X)$ est le logarithme de F_e.

2.1.4 Le logarithme des groupes formels de Lubin-Tate

Soit $F(X,Y)$ un groupe formel de Lubin-Tate sur $\mathbb{Z}_p$. Nous avons vu qu'il existe une unique série $\lambda_F(T) \in \mathbb{Q}_p[[T]]$ telle que

- $F(X,Y) = \lambda_F^{-1}(\lambda_F(X) + \lambda_F(Y))$ et
- $\lambda_F(T) \equiv T \pmod{\deg 2}$

appelée logarithme de F. Avec les notations des endomorphismes de groupes formels, on peut également écrire que $\lambda_F(T)$ est l'unique série de $\mathbb{Q}_p[[T]]$ vérifiant :

- $[p](T) = \lambda_F^{-1}(p\lambda_F(T))$ et
- $\lambda_F(T) \equiv T \pmod{\deg 2}$.

Soit $G_m(X,Y) = X + Y + XY$ le groupe multiplicatif sur $\mathbb{Z}_p$. Alors on a :

$$\lambda_{G_m}(T) = \log(1+T).$$

Soient maintenant $f \in \mathcal{F}_p$ et $G = F_f$ le groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ admettant $f(T)$ pour endomorphisme.

Lemme 2.1.2 *Le groupe formel G est isomorphe sur $\mathbb{Z}_p$ à G_m et un isomorphisme est*

$$\lambda_{G_m}^{-1} \circ \lambda_G(T) = \exp(\lambda_G(T)) - 1.$$

Preuve : On a

$$G_a = G_m^{\lambda_{G_m}} = \lambda_{G_m} \circ G_m \circ \lambda_{G_m}^{-1}$$

et

$$G_a = G^{\lambda_G} = \lambda_G \circ G \circ \lambda_G^{-1}.$$

D'où :

$$\lambda_{G_m} \circ G_m \circ \lambda_{G_m}^{-1} = \lambda_G \circ G \circ \lambda_G^{-1}$$

et

$$\lambda_{G_m}^{-1} \circ \lambda_G \circ G = G_m \circ \lambda_{G_m}^{-1} \circ \lambda_G.$$

Proposition 2.1.3 *Soit $g(T) = T + \sum_{i=2}^{\infty} b_i T^i \in \mathbb{Z}_p[[T]]$ et soit $\lambda(T) \in \mathbb{Q}_p[[T]]$ la solution de l'équation fonctionnelle*

$$\lambda(T) = g(T) + \frac{1}{p}\lambda(T^p).$$

Alors $\lambda(T)$ est le logarithme d'un groupe formel de Lubin-Tate sur $\mathbb{Z}_p$. Inversement, le logarithme d'un groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ est la solution d'une telle équation fonctionnelle.

Preuve : On prend $A = \mathbb{Z}_p$, $K = \mathbb{Q}_p$ et $\pi = p$ dans la proposition 2.1.2.

Remarque : Si $g(T) = \sum_{i=1}^{+\infty} b_i T^i \in \mathbb{Z}_p[[T]]$ avec $b_1 = 1$, alors $\lambda(T) = \sum_{i=1}^{+\infty} a_i T^i \in \mathbb{Q}_p[[T]]$ vérifie la relation de récurrence suivante :

$a_i = b_i$ si p ne divise pas i,

$a_i = b_i + \frac{1}{p} a_{i/p}$ si p divise i.

Proposition 2.1.4 *Soit* $\alpha(T) = \sum_{i=0}^{+\infty} \frac{T^{p^i}}{p^i}$ *et soit* $g(T) = \sum_{i=1}^{+\infty} b_i T^i \in \mathbb{Z}_p[[T]]$ *avec* $b_1 = 1$. *Alors le groupe formel de Lubin-Tate sur* $\mathbb{Z}_p$ *défini par* g *(au sens de la proposition précédente) admet pour logarithme la série :*

$$\lambda(T) = \sum_{i=1}^{+\infty} b_i \alpha(T^i).$$

Preuve : Soit $\lambda(T)$ le logarithme du groupe formel défini par g. Alors $\lambda(T)$ vérifie :

$$\lambda(T) = g(T) + \frac{1}{p}\lambda(T^p).$$

Calculons $\sum_{i=1}^{\infty} b_i \alpha(T^i) - \frac{1}{p}\lambda(T^p) = \sum_{i=1}^{\infty} \left(b_i \alpha(T^i) - \frac{1}{p} b_i \alpha(T^{ip}) \right)$. On a :

$$b_i \alpha(T^i) = b_i T^i + b_i \frac{T^{ip}}{p} + b_i \frac{T^{ip^2}}{p^2} + \ldots$$

puis

$$\frac{1}{p} b_i \alpha(T^{ip}) = b_i \frac{T^{ip}}{p} + b_i \frac{T^{ip^2}}{p^2} + b_i \frac{T^{ip^3}}{p^3} + \ldots$$

D'où $b_i \alpha(T^i) - \frac{1}{p} b_i \alpha(T^{ip}) = b_i T^i$. On en déduit $\sum_{i=1}^{\infty} \left(b_i \alpha(T^i) - \frac{1}{p} b_i \alpha(T^{ip}) \right) = g(T)$ et que $\lambda(T) = \sum_{i=1}^{\infty} b_i \alpha(T^i)$.

Corollaire 2.1.1 *Soit* $\alpha(T) = \sum_{i=0}^{+\infty} \frac{T^{p^i}}{p^i}$ *et soit* $g(T) = \sum_{i=1}^{+\infty} b_i T^i \in \mathbb{Z}_p[[T]]$ *avec* $b_1 = 1$. *Alors un isomorphisme sur* $\mathbb{Z}_p$ *du groupe formel de Lubin-Tate défini par* g *sur le groupe multiplicatif* G_m *est donné par la série :*

$$T \mapsto \exp(\lambda_G(T)) - 1 = \prod_{i=1}^{+\infty} \left(\exp(\alpha(T^i)) \right)^{b_i} - 1.$$

Preuve : C'est immédiat.

Ces propriétés serviront un peu plus loin à l'établissement de résultats d'algébricité sur l'exponentielle d'Artin-Hasse dont le paragraphe suivant rappelle la définition.

2.1.5 Les séries d'Artin-Hasse

Soit $q = p^f$ et soit K le corps des fractions de l'anneau des vecteurs de Witt à coefficients dans $\mathbb{F}_q$. On note A son anneau des entiers. Soit le groupe additif $TA[[T]]$, vu en tant que $\mathbb{Z}_p$-module et soit le groupe multiplicatif $1 + TA[[T]]$ vu en tant que $\mathbb{Z}_p$-module multiplicatif.
On note Δ le Frobenius de l'extension $K/\mathbb{Q}_p$ et on définit son action sur $K[[T]]$ de la manière suivante :
Pour $\phi(T) = \sum_{r=0}^{\infty} a_r T^r \in K[[T]]$, on pose :

$$\Delta\phi = \phi^{\Delta} = \sum_{r=0}^{+\infty} a_r^{\Delta} T^{pr}.$$

Soit $h(T)$ une série à coefficients dans l'anneau A.

Lemme 2.1.3 *Pour tout $m \geq 1$, la série $\dfrac{(h^{pm} - h^{\Delta m})}{pm}$ est à coefficients dans A.*

Preuve : Il suffit de vérifier le lemme pour $m = p^r$ et dans ce cas la démonstration se fait par récurrence sur r.

Définition 2.1.1 *Soit $\epsilon(T) \in 1 + TA[[T]]$. On définit la fonction "logarithme d'Artin-Hasse" l sur $1 + TA[[T]]$ comme suit :*

$$l(\epsilon) = \left(1 - \frac{\Delta}{p}\right) \log(\epsilon(T)).$$

Lemme 2.1.4 *La série $l(\epsilon)$ est une série sans terme constant et à coefficients dans A : $l(\epsilon) \in TA[[T]]$.*

Preuve : Soit $\epsilon(T) = 1 + h(T)$ où $h(T) \in TA[[T]]$. Pour p impair on a

$$\begin{aligned} l(\epsilon) &= \sum_{i=1}^{\infty} (-1)^{i-1} \frac{h^i}{i} - \frac{1}{p} \sum_{i=1}^{\infty} (-1)^{i-1} \frac{h^{\Delta i}}{i} \\ &= \sum_{(i,p)=1} (-1)^{i-1} \frac{h^i}{i} + \sum_{i=1}^{\infty} (-1)^{i-1} \frac{h^{pi} - h^{\Delta i}}{pi}. \end{aligned}$$

On conclut alors par le lemme précédent. Le cas $p = 2$ se vérifie de la même manière.

Notons que du lemme précédent et de l'égalité

$$l(\epsilon\eta) = l(\epsilon) + l(\eta),$$

où ϵ, $\eta \in 1 + TA[[T]]$, on peut déduire que la fonction l définit un homomorphisme du $\mathbb{Z}_p$-module multiplicatif $1 + TA[[T]]$ dans le $\mathbb{Z}_p$-module additif $TA[[T]]$.
Remarque : La série $l(1 + h(T))$ est différente de la série composée $l(1 + T) \circ h(T)$.

Définissons maintenant la fonction inverse de l, de $TA[[T]]$ dans $1 + TA[[T]]$. Pour ce faire, on utilise la série de Šafarevič [30] :

$$E(T) = \exp\left(\sum_{i=0}^{+\infty} \frac{T^{p^i}}{p^i}\right).$$

De l'égalité

$$E(T) = \prod_{(i,p)=1} (1 - T^i)^{-\frac{\mu(i)}{i}} \tag{2.4}$$

(voir [30]), il apparaît que la série $E(T)$ est une série à coefficients dans A et de terme constant égal à 1.

Posons maintenant pour $\phi \in TA[[T]]$:

$$E(\phi(T)) = \exp\left(\left(1 + \frac{\Delta}{p} + \frac{\Delta^2}{p^2} + ...\right)(\phi(T))\right).$$

Il est clair que la fonction E est multiplicative : si ϕ et ψ sont 2 séries de $TA[[T]]$, alors nous avons :

$$E(\phi + \psi) = E(\phi)E(\psi).$$

On appelle cette fonction la fonction exponentielle d'Artin-Hasse.

Lemme 2.1.5 *L'évaluation de la fonction E en $\Phi(T)$ est une série à coefficients dans A et est de terme constant égal à 1 : $E(\phi(T)) \in 1 + TA[[T]]$.*

Preuve : voir [33].

Lemme 2.1.6 *Les fonctions l et E sont inverses l'une de l'autre :*

$$E(l(\epsilon)) = \epsilon(T),\ l(E(\phi)) = \phi(T).$$

Preuve : De la définition de E et l, il vient :

$$E(l(\epsilon)) = \exp\left(1 + \frac{\Delta}{p} + \frac{\Delta^2}{p^2} + ...\right)\left(\left(1 - \frac{\Delta}{p}\right)\log\epsilon\right) = \exp\log\epsilon = \epsilon(T),$$

$$l(E(\phi)) = \left(1 - \frac{\Delta}{p}\right)\log E(\phi) = \left(1 - \frac{\Delta}{p}\right)\log\left(\exp\left(1 + \frac{\Delta}{p} + \frac{\Delta^2}{p^2} + ...\right)(\phi)\right)$$
$$= \left(1 - \frac{\Delta}{p}\right)\left(1 + \frac{\Delta}{p} + \frac{\Delta^2}{p^2} + ...\right)(\phi) = \phi(T).$$

Remarque : La série $E(\Phi(T))$ est différente de la série composée $E(T) \circ \Phi(T)$.

2.1.6 Isomorphismes algébriques

Caractérisation

Théorème 2.1.2 *Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$. Alors il existe un groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ (qui est unique) admettant pour logarithme la série formelle*

$$T \mapsto \lambda(T) = \log(1 + \gamma(T)).$$

Preuve : Soit $\epsilon(T) \in 1+T\mathbb{Z}_p[[T]]$. On a vu dans le paragraphe précédent que $l(\epsilon(T)) = (1 - \frac{\Delta}{p})\log(\epsilon(T))$. On en déduit que $l(1 + \gamma(T)) = \log(1 + \gamma(T)) - \frac{1}{p}\log(1 + \gamma(T^p))$ (sur $\mathbb{Z}_p$, Δ est l'identité).
D'après le lemme 2.1.4, $l(1+\gamma(T)) \in \mathbb{Z}_p[[T]]$ et on vérifie aisément que $l(1+\gamma(T)) \equiv T \pmod{T^2}$. Ainsi il apparaît que $\log(1 + \gamma(T))$ vérifie l'équation fonctionnelle

$$\lambda(T) = g(T) + \frac{1}{p}\lambda(T^p)$$

avec $g(T) = l(1+\gamma(T))$. On en déduit que $\log(1+\gamma(T))$ est le logarithme d'un groupe formel de Lubin-Tate sur $\mathbb{Z}_p$.

Théorème et interprétation p-automatique

Théorème 2.1.3 *Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ telle que sa projection dans $\mathbb{F}_p[[T]]$ soit algébrique sur $\mathbb{F}_p(T)$, soit $\lambda(T) = \log(1 + \gamma(T))$ et soit $u \in \mathbb{Z}_p$. Si l'on pose $f(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p$, les assertions suivantes sont équivalentes :*

(i) *$u \in \mathbb{Q}$,*

(ii) *La série $\widetilde{[u]}_{ff}(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : Par le lemme 2.1.2, la série $\exp(\lambda(T)) - 1 = \gamma(T)$ est un isomorphisme sur $\mathbb{Z}_p$ entre le groupe multiplicatif et le groupe formel de logarithme $\lambda(T)$. Comme $\gamma(T)$ est de réduction modulo p algébrique sur $\mathbb{F}_p(T)$, en appliquant la proposition 2.1.1, on obtient l'équivalence du théorème.

Remarquons maintenant que l'on peut interpréter ce résultat en termes d'automates : Pour tout élément $f(T) \in \mathcal{F}_p$ et toute unité p-adique u, on définit la suite $(\Delta_n)_{n\geq 0}$ par : (on pose $F_n = \sum_{i=0}^{n-1} \Delta_i$)

$$\begin{aligned} \Delta_0 &= uT \\ \Delta_n &= \frac{f(F_n(T)) - F_n(f(T))}{p^{n+1} - p} \bmod T^{n+2}. \end{aligned}$$

Les éléments $\Delta_n(T)$ sont de la forme $\Delta_n(T) = u_n T^{n+1}$ avec $u_n \in \mathbb{Z}_p$ pour tout $n \in \mathbb{N}$.

Théorème 2.1.4 *Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ de projection dans $\mathbb{F}_p[[T]]$ algébrique sur $\mathbb{F}_p(T)$, soit $\lambda(T) = \log(1+\gamma(T))$ et soit $u \in \mathbb{Z}_p$. On pose $f(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p$ et on définit la suite $(u_n)_n$ comme ci-dessus.*
Les assertions suivantes sont équivalentes :

(i) $u \in \mathbb{Q}$,

(ii) *Il existe un p-automate (fini) engendrant la suite $(\widetilde{u}_n)_n$ où $\widetilde{u}_n$ désigne la réduction modulo p de $u_n \in \mathbb{Z}_p$.*

Un cas particulier

Soient $p = 3$ et $f(T)$, $g(T) \in \mathcal{F}_3$ définis par $f(T) = (1+T)^3 - 1$ et $g(T) = 3T + T^3$. On prend $K = \mathbb{Q}_3$, $A = \mathbb{Z}_3$ et on pose

$$\begin{aligned} \mu(T) &= \frac{2T + T^2}{1+T} \\ &= 2T + \sum_{i=1}^{\infty} (-1)^i T^{i+1} \in \mathbb{Z}_3[[T]]. \end{aligned}$$

Lemme 2.1.7 *On a $\mu(T) \in Hom(F_f, F_g)$.*

Preuve : D'après la théorie de Lubin-Tate, pour tout $u \in U_3$ et tous $f(T)$ et $g(T)$ dans $\mathcal{F}_3$, il existe un unique élément $\nu(T) \in \mathrm{Hom}(F_f, F_g)$ vérifiant $\nu(T) \equiv uT \pmod{\deg 2}$ et $\nu(T) \in \mathbb{Z}_3[[T]]$. Il est caractérisé par :

$$\begin{cases} \nu(T) \equiv uT \pmod{\deg 2}, \\ \nu \circ f(T) = g \circ \nu(T). \end{cases}$$

La première condition est vérifiée par $\mu(T)$ pour $u = 2$.
De plus, $\mu \circ f(T) = (1+T)^3 - (1+T)^{-3} = g \circ \mu(T)$, d'où la deuxième condition.
Remarquons maintenant que le coefficient de T dans l'expression de $\mu(T)$ étant inversible dans $\mathbb{Z}_3$, la série $\mu(T)$ est réversible. Le calcul nous montre alors que

$$\mu^{-1}(T) = \frac{T - 2 + (4+T^2)^{1/2}}{2}$$

(notons qu'il faut comprendre par cette écriture le développement en série de $\mu^{-1}(T)$ en $T = 0$).

Lemme 2.1.8 *Pour tout $a \in A$, on a $[a]_{gg}(T) = \sum_{i=1}^{\infty} \alpha_i T^i$ avec $\alpha_1 = a$ et :*

$$\begin{aligned} \alpha_i &= 0 \text{ si } i \text{ est pair et} \\ \alpha_i &= \frac{a(a^2-1)(a^2-3)(a^2-5)\ldots(a^2-(i-2))}{4 \times 6 \times 8 \times 10 \times \ldots \times (2i)} \text{ si } i \text{ est impair.} \end{aligned}$$

Preuve : Il suffit d'écrire

$$\begin{aligned}[a]_{gg}(T) &= \mu \circ [a]_{ff} \circ \mu^{-1}(T) \\ &= \left(\frac{T+(4+T^2)^{1/2}}{2}\right)^a - \left(\frac{T+(4+T^2)^{1/2}}{2}\right)^{-a}\end{aligned}$$

et d'en prendre le développement en série.
Remarque : d'après la théorie des groupes formels de Lubin-Tate, la série obtenue est bien à coefficients dans $\mathbb{Z}_3$.

Proposition 2.1.5 *La série $[a]_{gg}(T)$ est un polynôme si et seulement si a est un entier impair et dans ce cas, $d^\circ([a]_{gg}(T)) = a$.*

Preuve : C'est évident à partir de l'écriture de $[a]_{gg}(T)$.

Proposition 2.1.6 *Soit $a \in \mathbb{Z}_3$. Les assertions suivantes sont équivalentes :*

(i) $a \in \mathbb{Q}$,

(ii) *La série $\widetilde{[a]}_{gg}(T)$ est algébrique sur $\mathbb{F}_3(T)$.*

Preuve : L'isomorphisme $\mu(T)$ entre les groupes formels F_f et F_g est de réduction modulo 3 appartenant à $\mathbb{F}_3(T)$ et donc de manière évidente algébrique sur $\mathbb{F}_3(T)$. On conclut grâce à la proposition 2.1.1.

Corollaire 2.1.2 *Soit $\alpha(a) = (\alpha_i)_{i\geq 1}$ la suite du lemme 2.1.8. La réduction modulo 3 de $\alpha(a)$ vérifie*

$$\widetilde{\alpha}(a) \text{ est 3-automatique} \Leftrightarrow a \in \mathbb{Q}.$$

Remarque : Il est possible d'établir une récurrence sur les coefficients de $[a]_{gg}(T)$: Définissons tout d'abord la suite $(\alpha'_i)_i$ par

$$\begin{aligned}\alpha'_1 &= \alpha_1 \\ \alpha'_i &= \alpha'_{i-1}\frac{(a-2i+1)(a+2i-1)}{4(2i)(2i+1)}.\end{aligned}$$

Si l'on écrit $[a]_{gg}(T) = \sum_{i=1}^{\infty} \alpha_i T^i$, on a alors

$$\begin{aligned}\alpha_1 &= a, \\ \alpha_i &= \alpha'_{(i+1)/2} \text{ si } i \text{ est impair}, \\ \alpha_i &= 0 \text{ si } i \text{ est pair}.\end{aligned}$$

2.2 Corps de normes des extensions de Lubin-Tate

2.2.1 Notations et construction

Soit K un corps local de corps résiduel k fini de cardinal une puissance q de p. On note A_K l'anneau des entiers de K et U_K le groupe des éléments inversibles de A_K. Enfin, π représente une uniformisante de A_K. On pose :

$$\mathcal{F}_\pi = \{f(T) \in A_K[[T]] | f(T) \equiv \pi T \pmod{\deg 2},\ f(T) \equiv T^q \pmod{\pi}\}$$

et on définit le groupe $\widetilde{\mathcal{F}} = \{f(T) \in k[[T]] | v_T(f) = 1\}$ muni de la loi de composition. Pour $\mu(T) \in \widetilde{\mathcal{F}}$, on définit l'application i_T par $i_T(\mu(T)) = v_T(\mu(T)T^{-1} - 1)$. On a $i_T(\mu(T)) = n \Leftrightarrow \mu(T) = T + \alpha_{n+1}T^{n+1} + \alpha_{n+2}T^{n+2} + ...$
Soient $f(T) \in \mathcal{F}_\pi$ et $F_f(X,Y)$ l'unique groupe formel de Lubin-Tate sur A_K admettant $f(T)$ pour endomorphisme. Si $\overline{K}$ désigne une clôture algébrique de K, on pose

$$\Lambda_n^f = \{\lambda \in \overline{K} | Ord(\lambda) > 0 \text{ et } f^n(\lambda) = 0\}.$$

On pose $\Lambda_\infty^f = \bigcup_{n\in\mathbb{N}} \Lambda_n^f$, puis pour tout $n \in \mathbb{N}$, $K_n = K(\Lambda_n^f)$. On note $L = K(\Lambda_1^f)$ et $L_\infty = K(\Lambda_\infty^f)$. L'extension L_∞/K est abélienne et totalement ramifiée. L'application de réciprocité $(\ , L_\infty/K)$ induit un isomorphisme $u \mapsto \sigma_u$ de U_K sur $Gal(L_\infty/K)$. Pour tout $n > 0$, désignons par $U_K^{(n)}$ le groupe formé des $u \in U_K$ tels que $v_K(u-1) \geq n$. Alors K_n est le corps des points fixes de L_∞ sous l'action de $(U_K^{(n)}, L_\infty/K)$. De plus, l'isomorphisme entre U_K et $Gal(L_\infty/K)$ est un isomorphisme de groupes filtrés. On en déduit que L_∞/K est *A.P.F.*. Si l'on désigne par $(K[i])_{i\geq -1}$ sa tour des sous-extensions élémentaires, on a :

$$\begin{aligned} K[i] &= K \text{ si } i = -1 \text{ ou } i = 0, \\ &= K_n \text{ si } q^{n-1} \leq i \leq q^n - 1. \end{aligned}$$

Les nombres inférieurs de ramification de l'extension L_∞/K sont les $q^n - 1$, pour $n > 0$. Posons pour tout $n > 0$:

- $r_n = \left(\dfrac{(p-1)(q^n-1)}{p}\right)$,
- $\overline{A}_n = A_{K_n}/P_{K_n}^{r_n}$.

La norme N_{K_{n+1}/K_n} induit, par passage au quotient, un homomorphisme surjectif $\overline{N}_n$: $\overline{A}_{n+1} \to \overline{A}_n$; on a $A_{X_K(L_\infty)} = \varprojlim \overline{A}_n$. Notons $\overline{\pi}_n$ l'image de π_n dans $\overline{A}_n$. Puisque $N_{K_{n+1}/K_n}(\pi_{n+1}) = (-1)^{q-1}\pi_n$, on a :

$$\overline{N}_n(\overline{\pi}_{n+1}) = (-1)^{q-1}\overline{\pi}_n.$$

Le calcul nous montre alors (voir [35]) que dans tous les cas (caractéristique quelconque et $p \geq 2$) :

$$\overline{N}_n(\overline{\pi}_{n+1}) = \overline{\pi}_n.$$

Il en résulte que la suite $(\overline{\pi}_n)_{n\geq 1}$ définit un élément $\widehat{\pi}$ de $A_{X_K(L_\infty)}$. Puisque les π_n sont des uniformisantes de K_n, $\widehat{\pi}$ est une uniformisante de $X_K(L_\infty)$.

2.2.2 Action de Galois

L'application $a \mapsto [a]_{ff}$ est un homomorphisme injectif de A_K dans $\mathrm{End}(F_f)$. La théorie de Lubin-Tate donne explicitement σ_u pour tout $u \in U_K$:

$$\sigma_u(\pi_n) = [u^{-1}]_{ff}(\pi_n).$$

Si l'on note $\widetilde{[u]}_{ff}(T)$ la série obtenue en projetant les coefficients de $[u]_{ff}(T)$ dans k, nous avons la proposition :

Proposition 2.2.1 (Wintenberger [35])
Pour tout $u \in U_K$, on a $\sigma_u(\widehat{\pi}) = \widetilde{[u^{-1}]}_{ff}(\widehat{\pi})$.

Par la suite, nous adopterons les notations suivantes : La série $\widetilde{[u^{-1}]}_{ff}(T)$ est la série obtenue en projetant les coefficients de $[u^{-1}]_{ff}(T)$ dans k. Lorsque cette dernière est interprétée en tant qu'élément de $Gal(L_\infty/K)$ via l'application de réciprocité d'Artin, nous la notons σ_u^f. Enfin, la réduction modulo p de σ_u^f est notée $\widetilde{\sigma}_u^f$.
En résumé :

$$\begin{aligned} \sigma_u^f(T) &= [u^{-1}]_{ff}(T), \\ \widetilde{\sigma}_u^f(T) &= \widetilde{[u^{-1}]}_{ff}(T). \end{aligned}$$

Notons $G = Gal(L_\infty/K)$. Alors si l'on représente par μ_n le groupe des racines $n^{\text{ièmes}}$ de 1, G est isomorphe à $\mu_{q-1} \times \mathbb{Z}_p^\infty$ si $car(K) = p$ et à $\mu_{q-1} \times \mathbb{Z}_p^\rho$ si $car(K) = 0$ où ρ est tel que $q = p^\rho$. Dans tous les cas, si l'on note $\mathcal{T}$ le sous-groupe de torsion de G, on a $\mathcal{T} \simeq \mu_{q-1}$. Soit $d \geq 2$ un diviseur de $q-1$. On définit $\mathcal{T}^{(d)}$ comme étant le sous-groupe d'ordre d de $\mathcal{T}$. Alors il est clair que $\mathcal{T}^{(d)}$ est isomorphe à μ_d. Posons $K_\infty^{(d)} = L_\infty^{\mathcal{T}^{(d)}}$, corps des points fixes de L_∞ sous l'action de $\mathcal{T}^{(d)}$.
Remarquons maintenant que l'extension $K_\infty^{(d)}/K$ est A.P.F. car $[L_\infty : K_\infty^{(d)}] = d < +\infty$ avec L_∞/K A.P.F. [36].
On introduit les notations suivantes :
$Y_f = X_K(L_\infty)$ et $X_f^{(d)} = X_K(K_\infty^{(d)})$. On pose également $X_f = X_f^{(q-1)}$. L'extension $Y_f/X_f^{(d)}$ est galoisienne et $Gal(Y_f/X_f^{(d)}) \simeq Gal(L_\infty/K_\infty^{(d)})$ [36].
Par construction, Y_f est isomorphe à $\mathbb{F}_q((T))$ et $X_f^{(d)}$ à $\mathbb{F}_q((\theta_d))$ où $\theta_d \in \mathbb{F}_q[[T]]$. Le groupe $\widetilde{\mathcal{F}}$ opère par substitution à droite sur Y_f et $X_f^{(d)}$. Pour $u \in U_K$, si $\widetilde{\sigma}_u^f$ représente l'automorphisme de Y_f issu de u par l'application de réciprocité, $\widetilde{\sigma}_{u,d}^f$ représente la restriction de $\widetilde{\sigma}_u^f$ a $X_f^{(d)}$.
De manière générale, toute série $\widetilde{\alpha}(T)$ représentera la série $\alpha(T) \in A_K[[T]]$ dont les coefficients ont été projetés dans le corps résiduel $k = \mathbb{F}_q$.

2.2.3 Résultats préliminaires sur les restrictions

Proposition 2.2.2 *Soit $Y_f = \mathbb{F}_q((T))$. Alors :*

$$X_f^{(d)} = \mathbb{F}_q\left(\left(N_{Y_f/X_f^{(d)}}(T)\right)\right).$$

Preuve : Montrons tout d'abord que $\mathbb{F}_q\left(\left(N_{Y_f/X_f^{(d)}}(T)\right)\right) \subset X_f^{(d)}$. Pour simplifier les notations, on pose $\widetilde{N}(T) = N_{Y_f/X_f^{(d)}}(T)$. Soit $\alpha \in \mathbb{F}_q\left(\left(\widetilde{N}(T)\right)\right)$ on a :

$$\alpha = \sum_{i=-n}^{+\infty} \alpha_i \widetilde{N}(T)^i.$$

Soit δ un générateur de μ_{q-1} et soit $\widetilde{\sigma} \in Gal(Y_f/X_f^{(d)})$. D'après l'application de réciprocité d'Artin, on peut écrire qu'il existe $k \in \{0, ..., d-1\}$ tel que

$$\widetilde{\sigma}(T) = \widetilde{[\delta^{k\frac{q-1}{d}}]}_{ff}(T).$$

Calculons l'action de $\widetilde{\sigma}$ sur α :

$$\begin{aligned} \widetilde{\sigma} * \alpha &= \alpha \circ \widetilde{\sigma}(T) = \sum_{i=-n}^{+\infty} \alpha_i \left(\widetilde{N} \circ \widetilde{\sigma}(T)\right)^i \\ &= \sum_{i=-n}^{+\infty} \alpha_i \left(\widetilde{N} \circ \widetilde{[\delta^{k\frac{q-1}{d}}]}_{ff}(T)\right)^i \end{aligned}$$

Remarquons maintenant que

$$\widetilde{N}(T) = \prod_{i=0}^{d-1} \widetilde{[\delta^{i\frac{q-1}{d}}]}_{ff}(T).$$

On en déduit que

$$\widetilde{N} \circ \widetilde{[\delta^{k\frac{q-1}{d}}]}_{ff}(T) = \prod_{i=0}^{d-1} \widetilde{[\delta^{(i+k)\frac{q-1}{d}}]}_{ff}(T) = \prod_{i=0}^{d-1} \widetilde{[\delta^{i\frac{q-1}{d}}]}_{ff}(T)$$

(car $\delta^{\frac{q-1}{d}n} = \delta^{\frac{q-1}{d}(n \bmod d)}$). On obtient donc $\widetilde{\sigma} * \alpha = \alpha$ et $\mathbb{F}_q\left(\left(N_{Y_f/X_f^{(d)}}(T)\right)\right) \subset X_f^{(d)}$. De plus, $v_T(N(T)) = d$. Donc $[\mathbb{F}_q((T)) : \mathbb{F}_q((\widetilde{N}(T)))]v_T(T) = d$. On en déduit que $[\mathbb{F}_q((T)) : \mathbb{F}_q((N(T)))] = d$ et que $\mathbb{F}_q\left(\left(N_{Y_f/X_f^{(d)}}(T)\right)\right) = X_f^{(d)}$.

Proposition 2.2.3 *Soit* $\widetilde{\Delta}_u^{(d)}(T) = N_{Y_f/X_f^{(d)}}\left(\widetilde{\sigma}_u^f(T)\right)$ *pour* $u \in U_K$. *Alors :*

$$\widetilde{\Delta}_1^{(d)} \circ \widetilde{\sigma}_u^f(T) = \widetilde{\sigma}_{u,d}^f \circ \widetilde{\Delta}_1^{(d)}(T).$$

Preuve : Soit δ un générateur de μ_{q-1}. Par définition :

$$\widetilde{\Delta}_u^{(d)}(T) = \prod_{i=0}^{d-1} \left(\widetilde{[\delta^{i\frac{q-1}{d}}]}_{ff} * \widetilde{\sigma}_u^f(T)\right) = \prod_{i=0}^{d-1} \widetilde{[u^{-1}\delta^{i\frac{q-1}{d}}]}_{ff}(T).$$

De plus,

$$\begin{aligned}\widetilde{\Delta}_1^{(d)} \circ \widetilde{\sigma}_u^f(T) &= \left(\prod_{i=0}^{d-1} \widetilde{[\delta^{i\frac{q-1}{d}}]}_{ff}(T)\right) \circ \widetilde{\sigma}_u^f(T) \\ &= \prod_{i=0}^{d-1} \widetilde{[\delta^{i\frac{q-1}{d}}u^{-1}]}_{ff}(T) = \widetilde{\Delta}_u^{(d)}(T).\end{aligned}$$

Or $N_{Y_f/X_f^{(d)}}\left(\widetilde{\sigma}_u^f(T)\right) \in \mathbb{F}_q[[\widetilde{\Delta}_1^{(d)}(T)]]$. Donc il existe $\gamma(T) \in \mathbb{F}_q[[T]]$ telle que

$$\widetilde{\Delta}_1^{(d)} \circ \widetilde{\sigma}_u^f(T) = \gamma \circ \widetilde{\Delta}_1^{(d)}(T).$$

On peut ensuite écrire que $\widetilde{\Delta}_1^{(d)} \circ \widetilde{\sigma}_u^f(T) = \widetilde{\sigma}_u^f * \widetilde{\Delta}_1^{(d)}(T)$. Il s'agit donc de l'action de l'automorphisme $\widetilde{\sigma}_u^f$ de Y_f sur l'uniformisante $\widetilde{\Delta}_1^{(d)}(T)$ de $X_f^{(d)}$. Ainsi la série $\gamma(T)$ correspond à l'automorphisme de $X_f^{(d)}$ défini par la restriction de $\widetilde{\sigma}_u^f$ à $X_f^{(d)}$.

Proposition 2.2.4 *Supposons que la série $N_{Y_f/X_f^{(d)}}(T)$ soit algébrique sur $\mathbb{F}_q(T)$. Les assertions suivantes sont équivalentes :*

(i) *La série $\widetilde{\sigma}_u^f(T)$ est algébrique sur $\mathbb{F}_q(T)$,*

(ii) *La série $\widetilde{\sigma}_{u,d}^f(T)$ est algébrique sur $\mathbb{F}_q(T)$.*

Preuve : On est ici dans le contexte de la proposition 1.5.2 avec $\alpha(T) = \widetilde{\sigma}_{u,d}^f(T)$, $\beta(T) = \widetilde{\Delta}_1^{(d)}(T)$ et $\gamma(T) = \widetilde{\sigma}_u^f(T)$.

2.3 Polynômes de Bell, polynômes de Chebyshev

Il s'avère que les polynômes de Bell et les polynômes de Chebyshev apparaissent dans le calcul des restrictions d'automorphismes à des sous-corps induisant un groupe de Galois isomorphe à un sous groupe du groupe des racines $(p-1)^{\text{ièmes}}$ de 1. Nous voyons dans ce paragraphe les définitions et caractéristiques de base concernant ces polynômes.

2.3.1 Polynômes de Bell

Définition 2.3.1 *Les polynômes de Bell [13] (exponentiels) partiels sont les polynômes $B_{n,k} = B_{n,k}(x_1, x_2, ..., x_{n-k+1})$ de la suite infinie d'indéterminées $x_1, x_2, ...$ définis par le développement en série double formelle :*

$$\begin{aligned}\Phi(T,u) &= \exp\left(u\sum_{m\geq 1}\frac{x_m}{m!}T^m\right) = \sum_{n,k\geq 0}\frac{B_{n,k}}{n!}T^n u^k \\ &= 1 + \sum_{n\geq 1}\left(\frac{T^n}{n!}\sum_{k=1}^{n} u^k B_{n,k}(x_1, x_2, ...)\right).\end{aligned}$$

Proposition 2.3.1 [13] *Pour tout entier k, on a :*

$$\frac{1}{k!}\left(\sum_{m\geq 1}\frac{x_m}{m!}T^m\right)^k = \sum_{n\geq k}\frac{B_{n,k}}{n!}T^n.$$

Proposition 2.3.2 [13] *Les polynômes de Bell sont à coefficients entiers, homogènes de degré k, de poids n et ont pour expression exacte :*

$$B_{n,k}(x_1, x_2, ..., x_{n-k+1}) = \sum \frac{n!}{c_1!c_2!...(1!)^{c_1}(2!)^{c_2}...}x_1^{c_1}x_2^{c_2}...$$

la sommation ayant lieu sur tous les entiers $c_1, c_2, c_3, ... \geq 0$, tels que :

$$\begin{aligned} c_1 + 2c_2 + 3c_3 + ... &= n \\ c_1 + c_2 + c_3 + ... &= k. \end{aligned}$$

Relation de récurrence : $kB_{n,k} = \sum_{l=k-1}^{n-1}\begin{pmatrix} n \\ l \end{pmatrix} x_{n-l}B_{l,k-1}$.

2.3.2 Polynômes de Chebyshev

Définition 2.3.2 *Pour tout $n \in \mathbb{N}$, on appelle polynômes de Chebyshev les polynômes $P_n(T) \in \mathbb{Z}[T]$ définis par la relation de récurrence :*
$P_0(T) = 0$, $P_1(T) = T$ *et*

$$P_{n+1}(T) = 2T\,P_n(T) - P_{n-1}(T).$$

Proposition 2.3.3 *Les polynômes $P_n(T)$ vérifient pour $n \in \mathbb{N}$:*

$$P_n(T) = \cosh(n \arg\cosh(T)).$$

Définition 2.3.3 *Soit $\lambda \in U_p$. On étend la définition des polynômes de Chebyshev à U_p en posant*

$$S_\lambda(T) = \cosh(\lambda \arg\cosh(T)) \in \mathbb{Z}_p[[T]].$$

On appellera cette série "série de Chebyshev".

Remarque : L'expression de $S_\lambda(T)$ sous forme de série est bien entendue issue du développement en série en $T = 0$. Nous ne justifierons pas ici le fait que les coefficients sont bien dans $\mathbb{Z}_p$. Cependant, on pourra s'en assurer un peu plus loin en remarquant que l'expression des $S_\lambda(T)$ est "pratiquement" celle des endomorphismes d'un groupe formel sur $\mathbb{Z}_p$.

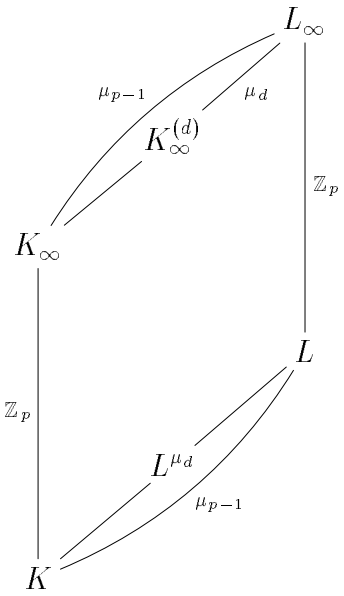
2.4 Automorphismes algébriques avec $car(K) = 0$

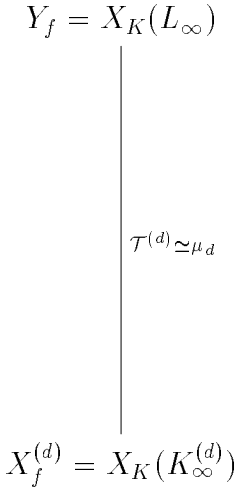
2.4.1 Notations

Soit p un nombre premier supérieur ou égal à 3. Soit le corps local $K = \mathbb{Q}_p$ de caractéristique 0 muni de sa valuation p-adique. On prend $\pi = p$, $A = \mathbb{Z}_p$ et $U = U_p$ muni de sa filtration : $U^{(n)} = 1 + p^n\mathbb{Z}_p$ pour tout $n \in \mathbb{N}$.
On pose

$$\mathcal{F}_p = \{f(T) \in \mathbb{Z}_p[[T]] | f(T) \equiv pT \pmod{\deg 2},\ f(T) \equiv T^p \pmod{p}\}$$

et on définit le groupe $\widetilde{\mathcal{F}} = \{f(T) \in \mathbb{F}_p[[T]] | v_T(f) = 1\}$ muni de la loi de composition. Pour $f(T) \in \mathcal{F}_p$, on définit L, L_∞, G, d, $\mathcal{T}$, $\mathcal{T}^{(d)}$, $K_\infty^{(d)}$, Y_f, $X_f^{(d)}$, $\widetilde{\sigma}_u^f$ et $\widetilde{\sigma}_{u,d}^f$ comme aux paragraphes 2.2.1 et 2.2.2.
On a $G \simeq \mu_{p-1} \times \mathbb{Z}_p$, $\mathcal{T} \simeq \mu_{p-1}$ et $\mathcal{T}^{(d)} \simeq \mu_d$.





2.4.2 Groupe formel des restrictions

Il se trouve que les restrictions $\widetilde{\sigma}_{u,d}^f$ peuvent être interprétées comme étant elles aussi les réductions modulo p d'endomorphismes $\sigma_{u,d}^f$ de groupes formels sur $\mathbb{Z}_p$ (qui quant à eux ne sont pas de Lubin-Tate).
Le but de cette partie est d'obtenir une expression du logarithme de ces groupes formels afin d'établir des formules explicites sur les restrictions.
On fixe f dans $\mathcal{F}_p$ et on emploie les notations suivantes :
Pour tout entier $n \geq 2$, on représente par $\pi(T)$ la série $\prod_{i=0}^{d-1}[\zeta^{-i}]_f f(T)$ où ζ est une racine primitive $d^{\text{ième}}$ de 1 dans $\mathbb{Z}_p$. La série $\pi(T)$ est telle que $\widetilde{\pi}(T) = N_{Y_f/X_f^{(d)}}(T)$.

La série $\pi \circ \sigma_u^f(T)$ est en fait une série en $\pi(T)$ à coefficients dans $\mathbb{Z}_p$. En effet, on a :

$$\begin{aligned} \pi \circ \sigma_u^f(T) &= \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \sigma_u^f(T) = \prod_{i=0}^{d-1} \sigma_{\zeta^i u}^f(T) \\ &= \prod_{i=0}^{d-1} \sigma_{u\zeta^i}^f(T) = \prod_{i=0}^{d-1} \sigma_u^f \circ \sigma_{\zeta^i}^f(T). \end{aligned}$$

Donc $\pi \circ \sigma_u^f(T)$ est une série en $(\sigma_1^f, \sigma_\zeta^f, \sigma_{\zeta^2}^f, ..., \sigma_{\zeta^{d-1}}^f)$ à coefficients dans $\mathbb{Z}_p$. Or,

$$\pi \circ \sigma_u^f(\sigma_\zeta^f(T)) = \prod_{i=0}^{d-1} \sigma_{\zeta^i u\zeta}^f(T) = \prod_{i=1}^{d} \sigma_{\zeta^i u}^f(T) = \pi \circ \sigma_u^f(T).$$

Donc les coefficients non nuls de $\pi \circ \sigma_u^f(T)$ sont les coefficients d'une puissance de $\sigma_1^f(T)\sigma_\zeta^f(T)...\sigma_{\zeta^{d-1}}^f(T)$ donc d'une puissance de $\pi(T)$.
Soit maintenant $\sigma_{u,d}^f(T)$ la série de $\mathbb{Z}_p[[T]]$ telle que :

$$\pi \circ \sigma_u^f(T) = \sigma_{u,d}^f \circ \pi(T).$$

Il vient :

$$\begin{aligned} \pi \circ \sigma_u^f(T) &= \left(\prod_{i=0}^{d-1} \sigma_{\zeta^i}^f(T) \right) \circ \sigma_u^f(T) \\ &= \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \sigma_u^f(T) \\ &= \sigma_{u,d}^f \circ \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f(T). \end{aligned}$$

Notons $\lambda(T)$ le logarithme du groupe formel de Lubin-Tate admettant $\sigma_p^f(T) \in \mathcal{F}_p$ pour endomorphisme et composons la dernière égalité à droite par $\lambda^{-1}(T)$. Il vient :

$$\prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \sigma_u^f \circ \lambda^{-1} = \sigma_{u,d}^f \circ \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}.$$

Par définition de $\lambda(T)$, on a $\lambda \circ \sigma_u^f(T) = (uT) \circ \lambda$. On en déduit $\sigma_u^f \circ \lambda^{-1}(T) = \lambda^{-1} \circ uT$. Doù :

$$\prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1} \circ uT = \sigma_{u,d}^f \circ \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}(T).$$

Lemme 2.4.1 *Il existe une série $g(T) \in \mathbb{Q}_p[[T]]$ telle que $g(T) \equiv T \pmod{\deg 2}$ et vérifiant $\prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}(T) = g\left((-1)^{d-1}T^d\right)$.*

Preuve : Posons $\alpha(T) = \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}(T)$. On a

$$\begin{aligned}
\alpha(\zeta T) &= \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}(\zeta T) \\
&= \prod_{i=0}^{d-1} \lambda^{-1} \circ \zeta^i T \circ \zeta T \\
&= \prod_{i=0}^{d-1} \lambda^{-1} \circ \zeta^{i+1} T \\
&= \prod_{i=0}^{d-1} \lambda^{-1} \circ \zeta^i T \\
&= \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}(\zeta T) \\
&= \alpha(T).
\end{aligned}$$

Donc il existe une série $\overline{g}(T)$ à coefficients dans $\mathbb{Q}_p[[T]]$ telle que $\alpha(T) = \overline{g}(T^d)$. De plus $\sigma_{\zeta^i}^f(T) \equiv \zeta^i T \pmod{\deg 2}$ et $\lambda^{-1}(T) \equiv T \pmod{\deg 2}$. On en déduit que

$$\prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1}(T) \equiv (-1)^{(d-1)} T^d \pmod{\deg\ d+1}.$$

Ainsi $\overline{g}(T^d) \equiv (-1)^{d-1} T^d \pmod{\deg\ d+1}$ et la série $g(T)$ cherchée est telle que

$$g((-1)^{d-1} T^d) = \overline{g}(T^d).$$

Théorème 2.4.1 *Il existe un groupe formel sur $\mathbb{Q}_p$ admettant les séries $\sigma_{u,d}^f(T)$ pour endomorphismes. Son logarithme $\overline{\lambda}(T)$ est donné par :*

$$\overline{\lambda}(\pi) = (-1)^{d-1} \left(\lambda(T)\right)^d.$$

Preuve : Le lemme précédent nous permet d'écrire :

$$g \circ (-1)^{d-1} T^d \circ uT = \sigma_{u,d}^f \circ g \circ (-1)^{d-1} T^d$$

puis

$$g \circ u^d T \circ (-1)^{d-1} T^d = \sigma_{u,d}^f \circ g \circ (-1)^{d-1} T^d$$

et :

$$g \circ u^d T = \sigma_{u,d}^f \circ g(T).$$

D'où $\sigma_{u,d}^f(T) = g \circ u^d T \circ g^{-1}(T)$ et ainsi on voit que $\overline{\lambda}(T) = g^{-1}(T)$.
Calculons $g\left((-1)^{d-1} T^d\right) \circ \lambda(T) = g \circ (-1)^{d-1} \left(\lambda(T)\right)^d$. On a

$$g\left((-1)^{d-1} T^d\right) \circ \lambda(T) = \prod_{i=0}^{d-1} \sigma_{\zeta^i}^f \circ \lambda^{-1} \circ \lambda(T) = \pi(T).$$

D'où $(-1)^{d-1}(\lambda(T))^d = g^{-1} \circ \pi(T)$ et

$$\overline{\lambda}(\pi) = (-1)^{d-1}(\lambda(T))^d .$$

Corollaire 2.4.1 *Il existe des groupes formels $F(X,Y)$ sur $\mathbb{Q}_p$ qui ne sont pas de Lubin-Tate et possédant un sous-groupe G de $End_{\mathbb{Q}_p}(F)$ d'endomorphismes qui sont à coefficients dans $\mathbb{Z}_p$ et tels que G est isomorphe à $\mathbb{Z}_p^{\times d} = \{u^d, u \in \mathbb{Z}_p\}$.*

Preuve : Si l'on considère les séries $\sigma_{u,d}^f(T)$, on sait que ces dernières sont à coefficients dans $\mathbb{Z}_p$. Ces séries sont les endomorphismes sur $\mathbb{Z}_p$ du groupe formel F du théorème 2.4.1.
Notons maintenant $\overline{\lambda}(T)$ le logarithme du groupe formel $F(X,Y)$. Il vient

$$\overline{\lambda} \circ \sigma_{u,d}^f(T) = u^d T \circ \overline{\lambda}(T)$$

puis

$$\sigma_{u,d}^f(T) = \overline{\lambda}^{-1} \circ u^d T \circ \overline{\lambda}(T) = [u^d](T),$$

d'où l'injection naturelle de $\mathbb{Z}_p^{\times d}$ dans $\mathrm{End}_{\mathbb{Q}_p}(F)$.

Corollaire 2.4.2 *Les séries $\sigma_{u,d}^f(T)$ sont en fait des puissances $d^{ièmes}$ de composition de séries à coefficients dans $\mathbb{Q}_p$.*

Preuve : Il vient $\sigma_{u,d}^f(T) = [u^{-d}](T) = \underbrace{[u^{-1}] \circ ... \circ [u^{-1}]}_{d \text{ fois}}(T)$, d'où le résultat.

Corollaire 2.4.3 *(Formule sommatoire des séries $\sigma_{u,d}^f(T)$)*
Soit $\lambda(T)$ le logarithme du groupe formel admettant $\sigma_p^f(T) \in \mathcal{F}_p$ pour endomorphisme et soit la série

$$\pi \circ \lambda^{-1}(T) = \sum_{n=1}^{+\infty} b_n \left((-1)^{d-1} T^d\right)^n .$$

Si l'on pose $\lambda_n = n! b_n$ et

$$\beta_n = \left(\sum_{k=1}^{n-1} (-1)^k B_{k+n-1,k}(0, \lambda_2, \lambda_3, ..., \lambda_n) \right)$$

où les $B_{n,k}$ sont les polynômes de Bell, alors :

$$\sigma_{u,d}^f(T) = \sum_{n=1}^{+\infty} \frac{1}{n!} \left(\sum_{k=1}^{n-1} \lambda_k u^{dk} B_{n,k}(\beta_1, \beta_2, ..., \beta_{n-k+1}) \right) T^n .$$

Preuve : D'après le théorème 2.4.1 :

$$\overline{\lambda}(\pi) = (-1)^{d-1}(\lambda(T))^d .$$

On en déduit que $\overline{\lambda}^{-1}\left((-1)^{d-1}T^d\right) = \pi \circ \lambda^{-1}(T) = \sum_{n=1}^{+\infty} b_n \left((-1)^{d-1}T^d\right)^n$. On peut ainsi écrire que

$$\overline{\lambda}^{-1}(T) = \sum_{n=1}^{+\infty} b_n T^n.$$

De plus, une reformulation de la formule de réversion des séries de Lagrange [13] nous permet d'affirmer que si

$$f(T) = \sum_{n=1}^{+\infty} \frac{f_n}{n!} T^n \in K[[T]],$$

alors son inverse pour la composition des séries s'écrit

$$f^{-1}(T) = \sum_{n=1}^{+\infty} \frac{\widetilde{f}_n}{n!} T^n$$

avec

$$\widetilde{f}_n = \sum_{k=1}^{n-1} (-1)^k f_1^{-n-k} B_{k+n-1,k}(0, f_2, f_3, ..., f_n) \text{ pour } n \geq 2 \text{ et } \widetilde{f}_1 = f_1^{-1}.$$

Si l'on pose $\lambda_n = n! b_n$, la série $\overline{\lambda}^{-1}(T)$ s'écrit

$$\overline{\lambda}^{-1}(T) = \sum_{n=1}^{+\infty} \frac{\lambda_n}{n!} T^n.$$

Il apparaît alors que

$$\overline{\lambda}(T) = \sum_{n=1}^{+\infty} \frac{\beta_n}{n!} T^n$$

avec

$$\beta_n = \sum_{k=1}^{n-1} (-1)^k B_{k+n-1,k}(0, \lambda_2, \lambda_3, ..., \lambda_n) \text{ (ici } \lambda_1 = 1).$$

Utilisons maintenant la formule de superposition de Faa di Bruno [13] qui permet d'écrire que si l'on a deux séries

$$f(T) = \sum_{k=1}^{+\infty} \frac{f_k}{k!} T^k$$

et

$$g(T) = \sum_{k=1}^{+\infty} \frac{g_k}{k!} T^k$$

alors la série composée $f \circ g(T)$ vérifie :

$$f \circ g(T) = \sum_{n=1}^{+\infty} \frac{h_n}{n!} T^n$$

avec

$$h_n = \sum_{k=1}^{n} f_k B_{n,k}(g_1, g_2, ..., g_{n-k+1}).$$

Il vient

$$\begin{aligned} \overline{\lambda}^{-1}\left(u^d \overline{\lambda}(T)\right) &= \left(\sum_{n=1}^{+\infty} \frac{\lambda_n}{n!} T^n\right) \circ u^d \overline{\lambda}(T) \\ &= \left(\sum_{n=1}^{+\infty} \frac{\lambda_n u^{nd}}{n!} T^n\right) \circ \left(\sum_{n=1}^{+\infty} \frac{\beta_n}{n!} T^n\right) \\ &= \left(\sum_{n=1}^{+\infty} \frac{\alpha_n}{n!} T^n\right) \circ \left(\sum_{n=1}^{+\infty} \frac{\beta_n}{n!} T^n\right) \end{aligned}$$

avec $\alpha_n = \lambda_n u^{nd}$. D'où :

$$\sigma_{u,d}^f(T) = \sum_{n=1}^{+\infty} \frac{1}{n!} \left(\sum_{k=1}^{n-1} \lambda_k u^{dk} B_{n,k}(\beta_1, \beta_2, ..., \beta_{n-k+1})\right) T^n.$$

Si l'on se place dans le cas de l'extension cyclotomique, alors $f(T) = (1+T)^p - 1$ et $\lambda(T) = \log(1+T)$. On en déduit que $\overline{\lambda}(\pi) = (-1)^{d-1} (\log(1+T))^d$, d'où $\overline{\lambda}((-1)^{d-1} T^d) = \pi \circ (e^T - 1)$.

Quelques calculs dans le cas où $\lambda(T) = \log(1+T)$:

Pour $d = 2$: $\pi(T) = ((1+T)-1)((1+T)^{-1} - 1)$. On trouve alors que $\overline{\lambda}^{-1}(-T^2) = 2 - 2\cosh(T)$ et

$$\overline{\lambda}(T) = -\left(\arg\cosh\left(\frac{2-T}{2}\right)\right)^2.$$

On en déduit que

$$\begin{aligned} \sigma_{u,2}^f(T) &= \overline{\lambda}^{-1} \circ u^2 T \circ \overline{\lambda}(T) \\ &= 2 - 2\cosh\left(u \arg\cosh\left(\frac{2-T}{2}\right)\right) \\ &= 2 - 2S_u\left(\frac{2-T}{2}\right) \end{aligned}$$

où $S_u(T)$ est la série de Chebyshev du paragraphe 2.3.2.

Pour $d = 3$: $\pi(T) = ((1+T)-1)\left((1+T)^j - 1\right)\left((1+T)^{j^2} - 1\right)$, d'où

$$\overline{\lambda}^{-1}(T^3) = 2\left(\sinh(T) + \sinh(jT) - \sinh((j+1)T)\right).$$

Pour $d = 4$: $\pi(T) = ((1+T)-1)\left((1+T)^{-1} - 1\right)\left((1+T)^i - 1\right)\left((1+T)^{-i} - 1\right)$, d'où

$$\overline{\lambda}^{-1}(-T^4) = \left(2 - 2\cosh(T)\right)\left(2 - 2\cosh(iT)\right).$$

2.4.3 Cas de l'extension cyclotomique

L'extension cyclotomique de $\mathbb{Q}_p$ est l'extension de Lubin-Tate définie par le groupe multiplicatif (sur $\mathbb{Z}_p$). Nous reformulons maintenant le théorème 2.1.1 en termes d'automorphismes de corps locaux en incluant en plus le cas des restrictions :

Théorème 2.4.2 *Soit $f(T) = (1+T)^p - 1$ et soit $a \in U_p$. Alors les assertions suivantes sont équivalentes :*

(i) $a \in \mathbb{Q}$,

(ii) *La série $\widetilde{\sigma}_a^f(T)$ est algébrique sur $\mathbb{F}_p(T)$,*

(iii) *La série $\widetilde{\sigma}_{a,2}^f(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : D'après le théorème 2.1.1, on a l'équivalence $(i) \Leftrightarrow (ii)$. Soit $X_f^{(2)}$ le sous-corps de Y_f tel que $Gal(Y_f/X_f^{(2)}) \simeq \mu_2$. On peut alors écrire que $Y_f = \mathbb{F}_p((T))$ et que $X_f^{(2)} = \mathbb{F}_p((\widetilde{\pi}))$ avec $\widetilde{\pi} = \widetilde{\pi}(T) = N_{Y_f/X_f^{(2)}}(T) = -\dfrac{T^2}{1+T}$ vu en tant qu'élément de $\mathbb{F}_p[[T]]$. On a :

$$\widetilde{\pi} \circ \widetilde{\sigma}_a^f(T) = \widetilde{\sigma}_{a,2}^f \circ \widetilde{\pi}(T)$$

Comme la série $\widetilde{\pi}(T)$ est dans $\mathbb{F}_p(T)$, elle est a fortiori algébrique sur $\mathbb{F}_p(T)$. Par la proposition 2.2.4, on en déduit que l'algébricité de $\widetilde{\sigma}_a^f(T)$ est équivalente à l'algébricité de $\widetilde{\sigma}_{a,2}^f(T)$.

Remarque : Si $d \geq 3$, la série $N_{Y_f/X_f^{(d)}}(T)$ est en général transcendante sur $\mathbb{F}_p(T)$.

Corollaire 2.4.4 *Soit $\lambda \in U_p$ et soit $u^{(\lambda)} = \left(u_k^{(\lambda)}\right)_{k\geq 0}$ la suite à coefficients dans $\mathbb{Z}_p$ définie par :*

$$u_k^{(\lambda)} = (-1)^{k+1} \left(\begin{array}{c} \lambda + k \\ \lambda - k \end{array} \right) \frac{2\lambda}{\lambda + k} \in \mathbb{Z}_p.$$

On définit la suite $\widetilde{u^{(\lambda)}} = \left(\widetilde{u_k^{(\lambda)}}\right)_{k\geq 0}$ comme étant la réduction modulo p de la suite $\left(u_k^{(\lambda)}\right)_{k\geq 0}$. Les assertions suivantes sont équivalentes :

(i) $\lambda \in \mathbb{Q}$,

(ii) *La suite $\widetilde{u^{(\lambda)}}$ est p-automatique.*

Preuve : Un calcul de Salinier et al. [25] montre que la série $\sigma_{\lambda,2}^f(T)$ s'écrit, pour $f(T) = (1+T)^p - 1$:

$$\sigma_{\lambda,2}^f(T) = \sum_{k=0}^{+\infty} u_k^{(\lambda)} T^k.$$

Par le théorème précédent, $\widetilde{\sigma}_{\lambda,2}^f(T)$ est algébrique si et seulement si λ est rationnel. Donc la suite $\left(\widetilde{u^{(\lambda)}}_k\right)_{k\geq 0}$ est p-automatique si et seulement si $\lambda \in \mathbb{Q}$.

Corollaire 2.4.5 *Soit $\lambda \in U_p$ et soit $S_\lambda(T)$ la série de Chebyshev associée à λ. Si l'on note $\widetilde{S_\lambda}(T)$ la réduction modulo p de $S_\lambda(T)$, alors les assertions suivantes sont équivalentes :*

(i) $\lambda \in \mathbb{Q}$,

(ii) *La série $\widetilde{S_\lambda}(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : On a vu que $\sigma^f_{\lambda,2}(T) = 2 - 2S_\lambda\left(\frac{2-T}{2}\right)$. On en déduit que

$$S_\lambda(T) = 1 - \frac{1}{2}\sigma^f_{\lambda,2}(2-T).$$

Il apparaît ainsi clairement, en vertu de la proposition 1.5.3, que $\widetilde{S_\lambda}(T)$ est algébrique si et seulement si la série $\widetilde{\sigma}^f_{\lambda,2}(T)$ est algébrique.

2.4.4 Cas général

Lemme 2.4.2 *Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ de projection dans $\mathbb{F}_p[[T]]$ algébrique sur $\mathbb{F}_p(T)$ et soit $\lambda(T) = \log(1+\gamma(T))$. On pose $g(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p$. Alors $N_{Y_g/X_g^{(2)}}(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : Soit $f(T) = (1+T)^p - 1$. On a

$$N_{Y_g/X_g^{(2)}}(T) = \widetilde{\sigma}^g_1(T)\widetilde{\sigma}^g_{-1}(T) = \widetilde{\mu}^{-1} \circ \widetilde{\sigma}^f_1 \circ \widetilde{\mu}(T) \times \widetilde{\mu}^{-1} \circ \widetilde{\sigma}^f_{-1} \circ \widetilde{\mu}(T)$$

avec $\widetilde{\mu}(T) = \widetilde{\gamma}(T)$ algébrique. De plus, comme 1 et $-1 \in U_p \cap \mathbb{Q}$, les séries $\widetilde{\sigma}^f_1(T)$ et $\widetilde{\sigma}^f_{-1}(T)$ sont algébriques. On en déduit que $N_{Y_g/X_g^{(2)}}(T)$ est algébrique sur $\mathbb{F}_p(T)$.

Théorème 2.4.3 *Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ telle que sa projection dans $\mathbb{F}_p[[T]]$ soit algébrique sur $\mathbb{F}_p(T)$, soit $\lambda(T) = \log(1+\gamma(T))$ et soit $a \in U_p$. On pose $g(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p$. Les assertions suivantes sont équivalentes :*

(i) $a \in \mathbb{Q}$,

(ii) *La série $\widetilde{\sigma}^g_a(T)$ est algébrique sur $\mathbb{F}_p(T)$,*

(iii) *$\widetilde{\sigma}^g_{a,2}(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : L'équivalence $(i) \Leftrightarrow (ii)$ est démontrée dans le théorème 2.1.3. Par le lemme précédent, l'algébricité de $N_{Y_g/X_g^{(2)}}(T)$ nous place dans le contexte de la proposition 2.2.4 et on en déduit l'équivalence $(ii) \Leftrightarrow (iii)$.

Interprétons ce résultat en termes de suites p-automatiques :
Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ de projection dans $\mathbb{F}_p[[T]]$ algébrique sur $\mathbb{F}_p(T)$ et soit

$\lambda(T) = \log(1+\gamma(T))$. On pose $f(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p$, $\pi(T) = \sigma_1^f(T)\sigma_{-1}^f(T)$ et on définit la suite $(b_n)_{n\geq 0}$ par

$$\pi \circ \lambda^{-1}(T) = \sum_{n=1}^{+\infty} b_n \left((-1)^{d-1}T^d\right)^n.$$

Théorème 2.4.4 *Soit $u \in U_p$. Pour $n \in \mathbb{N}$, on pose $\lambda_n = n!b_n$,*

$$\beta_n = \sum_{k=1}^{n-1}(-1)^k B_{k+n-1,k}(0, \lambda_2, \lambda_3, ..., \lambda_n)$$

et

$$\alpha_n = \sum_{k=1}^{n-1} \lambda_k u^{2k} B_{n,k}(\beta_1, \beta_2, ..., \beta_{n-k+1}) \bmod p.$$

Les assertions suivantes sont équivalentes :

(i) $u \in \mathbb{Q}$,

(ii) *La suite $(\alpha_n)_{n\geq 0}$ est p-automatique.*

Remarque : Dans le cas où $f(T) = pT + T^p$ avec $p = 3$, nous avons vu que les endomorphismes $[a]_{ff}(T)$ du groupe formel $F_f(X,Y)$ sont de la forme

$$[a]_{ff}(T) = \left(\frac{T + (4+T^2)^{1/2}}{2}\right)^a - \left(\frac{T + (4+T^2)^{1/2}}{2}\right)^{-a}.$$

Posons $\alpha(T) = \dfrac{T + (4+T^2)^{1/2}}{2}$ et notons $\widetilde{\sigma}_a^f(T) = [a]_{ff}(T) \bmod p$ l'automorphisme du corps de normes Y_f de l'extension maximale abélienne totalement ramifiée correspondante. Il vient :

$$\pi(T) = N_{Y_f/X_f^{(2)}}(T) = \widetilde{\sigma}_1(T)\widetilde{\sigma}_{-1}(T) = -T^2.$$

De l'expression $\sigma_a^f(T) = \alpha(T)^a - \alpha(T)^{-a}$, il vient $\sigma_a^f(T) = 2\sinh(a\log(\alpha(T)))$. Or $\sigma_a^f(T) = \lambda^{-1}(a\lambda(T))$ où $\lambda(T)$ désigne la logarithme du groupe formel $F_f(X,Y)$. On en déduit que $\lambda^{-1}(T) = 2\sinh(T/2)$. Le logarithme $\overline{\lambda}(T)$ du groupe formel des restrictions vérifie alors, d'après le théorème 2.4.1 :

$$\begin{aligned}
\overline{\lambda}^{-1}(-T^2) &= -4\sinh^2(T/2) \\
&= -4\left(\frac{e^T - e^{-T}}{2}\right)^2 \circ (T/2) \\
&= -2\cosh(T) + 2
\end{aligned}$$

Il vient $\overline{\lambda}(T) = -\left(\operatorname{arg\,cosh}\left(\dfrac{2-T}{2}\right)\right)^2$.

Les carrés de composition d'endomorphismes du groupe formel de logarithme $\overline{\lambda}(T)$ sont les séries $\sigma^f_{a,2}(T)$, séries dont la réduction modulo p donne les restrictions $\widetilde{\sigma}^f_{a,2}(T)$ des automorphismes $\widetilde{\sigma}^f_a(T)$. Nous avons :

$$\begin{aligned}\sigma^f_{a,2}(T) &= \overline{\lambda}^{-1} \circ a^2 T \circ \overline{\lambda}(T) \\ &= 2 - 2\cosh\left(a \arg\cosh\left(\frac{2-T}{2}\right)\right) \\ &= 2 - 2S_a\left(\frac{2-T}{2}\right)\end{aligned}$$

où $S_a(T)$ est la série de Chebyshev du paragraphe 2.3.2 associée à a.
En d'autres termes, dans le cas $p = 3$, si l'on note $\widetilde{\sigma}'_a(T)$ les automorphismes du corps de normes de l'extension cyclotomique de $\mathbb{Q}_p$, les restrictions $\widetilde{\sigma}'_{a,2}(T)$ coïncident avec les restrictions $\widetilde{\sigma}^f_{a,2}(T)$ des automorphismes $\widetilde{\sigma}^f_a(T)$.

2.5 Automorphismes algébriquement indépendants

2.5.1 Résultats préliminaires

Dans cette partie, K représente un corps quelconque.

Lemme 2.5.1 *Soit $U = \{u_1(T), ..., u_n(T)\}$ une famille de séries dans $K[[T]]$ de valuation T-adique égale à 1 et soit $\mu(T) \in K[[T]]$ de valuation T-adique supérieure ou égale à 1 et algébrique sur $K(T)$. Si l'on note U' la famille des séries $u_i \circ \mu(T)$ pour $i = 1, ..., n$ alors les assertions suivantes sont équivalentes :*

(i) *La famille U est une base de transcendance de l'extension $K(T,U)/K(T)$,*

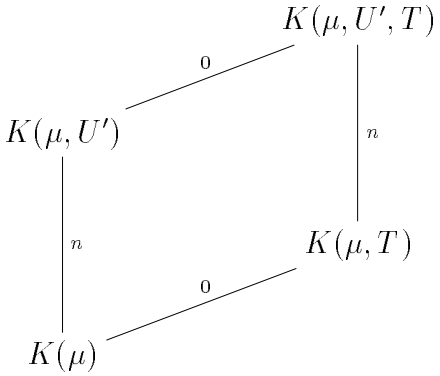
(ii) *La famille U' est une base de transcendance de l'extension $K(T,U')/K(T)$.*

Preuve : Supposons que la famille U soit une base de transcendance de l'extension $K(T,U)/K(T)$. Le degré de transcendance de $K(T,U)/K(T)$ est alors n. La série $\mu(T)$ étant de valuation T-adique supérieure ou égale à 1, on peut pratiquer le transport de structure $T \to \mu(T)$ ($\mu(T)$ se comporte comme la variable formelle T sur le corps K). On obtient $deg.tr_{K(\mu)}K(\mu,U') = n$. Comme $\mu(T)$ est algébrique sur $K(T)$, on peut affirmer que T est algébrique sur $K(\mu(T))$ et donc sur $K(\mu(T),U')$.
On obtient ainsi dans un premier temps :

$$\begin{aligned} deg.tr_{K(\mu)}K(\mu,U',T) &= deg.tr_{K(\mu,U')}K(\mu,U',T) + deg.tr_{K(\mu)}K(\mu,U') \\ &= 0 + n \\ &= n \end{aligned}$$

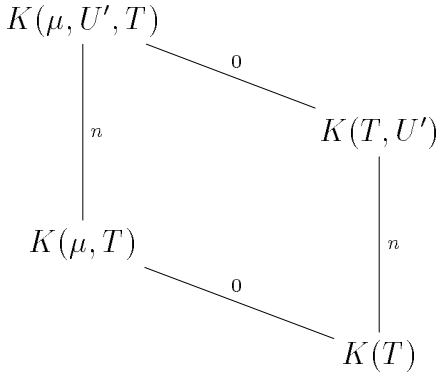
puis dans un deuxième temps :

$$\begin{aligned} deg.tr_{K(\mu,T)}K(\mu,U',T) &= deg.tr_{K(\mu)}K(\mu,U',T) - deg.tr_{K(\mu)}K(\mu,T) \\ &= n - 0 \\ &= n \end{aligned}$$



De plus, la série $\mu(T)$ étant algébrique sur $K(T)$, l'extension $K(\mu, U', T)/K(U', T)$ est algébrique et $deg.tr_{K(U',T)}K(\mu, U', T) = 0$. De même, $deg.tr_{K(T)}K(\mu(T), T) = 0$. On en déduit que $deg.tr_{K(T)}K(\mu, U', T) = n + 0 = n$. D'où

$$\begin{array}{rcccc} deg.tr_{K(T)}K(U', T) & = & deg.tr_{K(T)}K(\mu, U', T) & - & deg.tr_{K(U',T)}K(\mu, U', T) \\ & = & n & - & 0 \\ & = & n & & \end{array}$$



Comme U' contient n éléments, on en déduit que c'est une base de transcendance de $K(U', T)/K(T)$.

Supposons maintenant que la famille U' soit base de transcendance de l'extension $K(U', T)/K(T)$.
On a $deg.tr_{K(T)}K(U', T) = n$. La série $\mu(T)$ étant algébrique sur $K(T)$, on en déduit que

$$deg.tr_{K(T,U')}K(U', T, \mu) = 0$$

et que

$$deg.tr_{K(T)}K(\mu, T) = 0.$$

D'où

$$\begin{array}{rcccc} deg.tr_{K(T)}K(U', T, \mu) & = & deg.tr_{K(T,U')}K(\mu, U', T) & + & deg.tr_{K(T)}K(U', T) \\ & = & 0 & + & n \\ & = & n & & \end{array}$$

Ainsi :

$$\begin{array}{rcccc} deg.tr_{K(T,\mu)}K(\mu,U',T) & = & deg.tr_{K(T)}K(\mu,U',T) & - & deg.tr_{K(T)}K(\mu,T) \\ & = & n & - & 0 \\ & = & n & & \end{array}$$

L'algébricité de $\mu(T)$ sur $K(T)$ étant équivalente à celle de T sur $K(\mu(T))$, on a :

$$deg.tr_{K(U',\mu)}K(\mu,T,U') = 0$$

et

$$deg.tr_{K(\mu)}K(\mu,T) = 0.$$

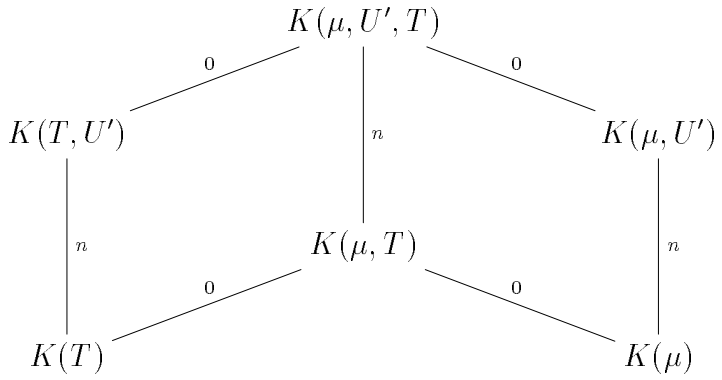
D'où :

$$\begin{array}{rcccc} deg.tr_{K(\mu)}K(\mu,U',T) & = & deg.tr_{K(T,\mu)}K(\mu,U',T) & + & deg.tr_{K(\mu)}K(\mu,T) \\ & = & n & + & 0 \\ & = & n & & \end{array}$$

Donc

$$\begin{array}{rcccc} deg.tr_{K(\mu)}K(\mu,U') & = & deg.tr_{K(\mu)}K(\mu,U',T) & - & deg.tr_{K(\mu,U')}K(\mu,T,U') \\ & = & n & - & 0 \\ & = & n & & \end{array}$$

Par transport de structure $\mu \to T$, on conclut que $deg.tr_{K(T)}K(T,U) = n$, ce qui est équivalent à dire que U est une base de transcendance de l'extension $K(T,U)/K(T)$.



Lemme 2.5.2 *Soit $V = \{v_1(T), ..., v_n(T)\}$ une famille de séries dans $K[[T]]$ de valuation T-adique égale à 1 et soit $\mu(T) \in K[[T]]$ de valuation T-adique supérieure ou égale à 1 et algébrique sur $K(T)$. Si l'on note V' la famille des séries $\mu \circ v_i(T)$ pour $i = 1, ..., n$ alors les assertions suivantes sont équivalentes :*

(i) *La famille V est une base de transcendance de l'extension $K(T,V)/K(T)$,*

(ii) *La famille V' est une base de transcendance de l'extension $K(T,V')/K(T)$.*

Preuve : Supposons que la famille V soit une base de transcendance de l'extension $K(T,V)/K(T)$. On a

$$deg.tr_{K(T)}K(T,V) = n.$$

On sait que l'extension $K(T,\mu(T))/K(T)$ est algébrique. Par transport de structure $T \to v_i(T)$ (la valuation T-adique de $v_i(T)$ est égale à 1), on peut affirmer que l'extension $K(v_i, \mu \circ v_i)/K(v_i)$ est algébrique pour tout $i = 1, ..., n$. On en déduit que l'extension $K(V,V')/K(V)$ est algébrique. D'où

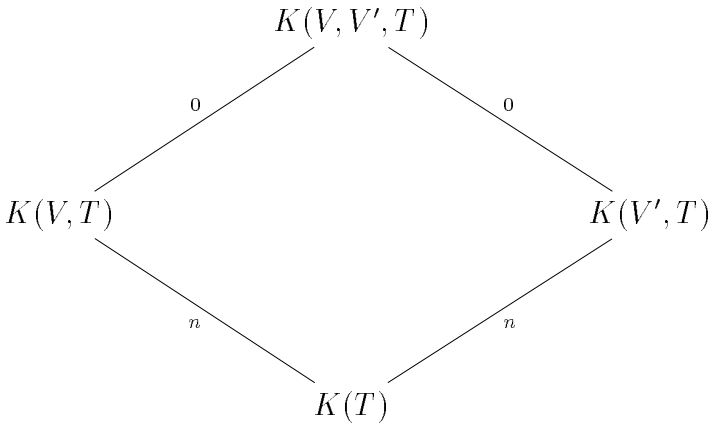
$$K(V,V',T)/K(V,T) \text{ est algébrique.}$$

Il vient alors :

$$\begin{array}{rcccc} deg.tr_{K(T)}K(V,V',T) & = & deg.tr_{K(V,T)}K(V,V',T) & + & deg.tr_{K(T)}K(V,T) \\ & = & 0 & + & n \\ & = & n & & \end{array}$$

Comme $\mu(T)$ est algébrique sur $K(T)$, on a vu qu'on pouvait écrire que T est algébrique sur $K(\mu)$ et l'extension $K(T,\mu)/K(\mu)$ est algébrique.
Par transport de structure $T \to v_i$, il vient $K(v_i, \mu \circ v_i)/K(\mu \circ v_i)$ est algébrique pour $i = 1, ..., n$. D'où $K(V,V')/K(V')$ est algébrique et donc $K(V,V',T)/K(V',T)$ également.
Ainsi :

$$\begin{array}{rcccc} deg.tr_{K(T)}K(V',T) & = & deg.tr_{K(T)}K(V',V,T) & - & deg.tr_{K(V',T)}K(V',V,T) \\ & = & n & - & 0 \\ & = & n & & \end{array}$$



La famille V' étant de cardinal n, on en déduit qu'elle est base de transcendance de $K(V',T)/K(T)$.

Supposons maintenant que la famille V' soit base de transcendance de l'extension $K(V',T)/K(T)$. Il vient

$$deg.tr_{K(T)}K(V',T) = n.$$

L'extension $K(T,\mu(T))/K(T)$ étant algébrique, on peut écrire, par transport de structure $T \to v_i$, que $K(v_i,\mu\circ v_i)/K(v_i)$ est algébrique. On en déduit que $K(V,V')/K(V)$ est algébrique puis que $K(T,V,V')/K(T,V)$ l'est aussi.
Comme l'extension $K(T,\mu)/K(\mu)$ est algébrique, il vient :

$$K(v_i,\mu\circ v_i)/K(\mu\circ v_i) \text{ est algébrique}$$

et donc de même pour $K(V,V')/K(V')$ et $K(V,V',T)/K(V',T)$.
On a alors :

$$\begin{array}{rcccc} deg.tr_{K(T)}K(V,V',T) & = & deg.tr_{K(V',T)}K(V,V',T) & + & deg.tr_{K(T)}K(V',T) \\ & = & 0 & + & n \\ & = & n & & \end{array}$$

$$\begin{array}{rcccc} deg.tr_{K(T)}K(V,T) & = & deg.tr_{K(T)}K(V,V',T) & - & deg.tr_{K(T,V)}K(V',V,T) \\ & = & n & - & 0 \\ & = & n & & \end{array}$$

On en déduit que V est base de transcendance de l'extension $K(T,V)/K(T)$.

Proposition 2.5.1 *Soient $U=\{u_1(T),...,u_n(T)\}$ et $V=\{v_1(T),...,v_n(T)\}$ deux familles de séries dans $K[[T]]$ de valuation T-adique égale à 1. Supposons qu'il existe $\mu(T)\in K[[T]]$ de valuation T-adique supérieure ou égale à 1, algébrique sur $K(T)$ et vérifiant*

$$u_i\circ\mu(T)=\mu\circ v_i(T) \text{ pour } i=1,...,n.$$

Les assertions suivantes sont alors équivalentes :

(i) *La famille U est algébriquement indépendante sur $K(T)$,*

(ii) *La famille V est algébriquement indépendante sur $K(T)$.*

Preuve : On reprend les notations U' et V' des deux lemmes précédents. Supposons que la famille U soit algébriquement indépendante sur $K(T)$. Ceci est équivalent à dire que la famille U est une base de transcendance de l'extension $K(T,U)/K(T)$. D'après le lemme 2.5.1, on en déduit que c'est équivalent à dire que U' est une base de transcendance de l'extension $K(T,U')/K(T)$. De plus, il est clair que, d'après les propriétés de $\mu(T)$, les familles U' et V' sont la même famille. On a alors les équivalences suivantes :

- La famille U est algébriquement indépendante sur $K(T)$,
- La famille V' est une base de transcendance de $K(V',T)/K(T)$,
- La famille V est une base de transcendance de $K(V,T)/K(T)$ (lemme 2.5.2),
- La famille V est algébriquement indépendante sur $K(T)$.

2.5.2 Condition nécessaire et suffisante

On rappelle que l'ensemble $\mathcal{F}_p$ est défini par :

$$\mathcal{F}_p = \{f(T) \in \mathbb{Z}_p[[T]] | f(T) \equiv pT \pmod{\deg 2},\ f(T) \equiv T^p \pmod{p}\}$$

Théorème 2.5.1 *Soit une série $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ telle que sa projection dans $\mathbb{F}_p[[T]]$ soit algébrique sur $\mathbb{F}_p(T)$ et soit $\lambda(T) = \log(1+\gamma(T))$.*
Soient $\lambda_1, ..., \lambda_n \in U_p$. Si l'on pose

$$f(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p,$$

les assertions suivantes sont équivalentes :

(i) *Les éléments 1, λ_1,...,λ_n sont $\mathbb{Z}$-linéairement indépendants,*

(ii) *Les séries $\widetilde{\sigma}^f_{\lambda_i}(T)$, $i = 1, ..., n$ sont algébriquement indépendantes sur $\mathbb{F}_p(T)$.*

Preuve : Le résultat ci-dessus est connu lorsque $\gamma(T) = T$, ce qui correspond à $f_0(T) = (1+T)^p - 1$ (voir théorème 1.4.3). Les séries $\widetilde{\sigma}^{f_0}_{\lambda_i}(T)$ correspondantes sont les réductions modulo p des endomorphismes du groupe multiplicatif sur $\mathbb{Z}_p$, c'est-à-dire les $(1+T)^{\lambda_i} - 1 \bmod p$. En fait, le résultat est établi pour les séries $(1+T)^{\lambda_i}$ prises hors contexte de la théorie de Lubin-Tate, mais il est clair que, modulo p, les $(1+T)^{\lambda_i}$ pour $i = 1, ..., n$ sont algébriquement indépendantes sur $\mathbb{F}_p(T)$ si et seulement si les $(1+T)^{\lambda_i} - 1$, $i = 1, ..., n$ le sont. On peut ainsi se rattacher aux endomorphismes de groupes formels de Lubin-Tate.
D'après le paragraphe 2.1.6, on sait qu'il existe $\mu(T) \in \mathbb{Z}_p[[T]]$ vérifiant

$$f \circ \mu(T) = \mu \circ f_0(T)$$

et étant de projection $\widetilde{\mu}(T)$ dans $\mathbb{F}_p[[T]]$ algébrique sur $\mathbb{F}_p(T)$ (en fait $\mu(T) = \gamma^{-1}(T)$). Il vient alors :

$$\widetilde{\sigma}^f_{\lambda_i} \circ \widetilde{\mu}(T) = \widetilde{\mu} \circ \widetilde{\sigma}^{f_0}_{\lambda_i}(T).$$

D'après la proposition 2.5.1, avec $K = \mathbb{F}_p$, l'indépendance algébrique des $\widetilde{\sigma}^f_{\lambda_i}(T)$ est équivalente à celle des $\widetilde{\sigma}^{f_0}_{\lambda_i}(T)$, d'où la conclusion.
Exemple : Soit $a \in \mathbb{Z}_p$ non nul et soit

$$f(T) = \frac{1}{a}\left(a(1+T+aT^2)^p + 1/4 - a\right)^{1/2} - \frac{1}{2}a.$$

Le calcul montre que $f(T) \in \mathbb{Z}_p[[T]]$ et que l'on a $f(T) \equiv pT \pmod{\deg 2}$ et $f(T) \equiv T^p \pmod{p}$. En d'autres termes, $f(T) \in \mathcal{F}_p$. Il existe donc un unique groupe formel $F_f(X,Y)$ de Lubin-Tate sur $\mathbb{Z}_p$ tel que $f(T) \in \mathrm{End}(F_f)$. Soit $\alpha \in \mathbb{Z}_p$. Les assertions suivantes sont équivalentes :

(i) $\alpha \in \mathbb{Q}$,

(ii) La série $\widetilde{[\alpha]}_{ff}(T)$ est algébrique sur $\mathbb{F}_p(T)$.

En effet, si l'on prend, dans le théorème 2.1.3, $\gamma(T) = T + aT^2$, il est clair que la réduction $\widetilde{\gamma}(T)$ modulo p de $\gamma(T)$ est algébrique sur $\mathbb{F}_p(T)$. Soit $F(X,Y)$ le groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ admettant la série $\lambda(T) = \log(1+\gamma(T))$ pour logarithme. On a

$$\lambda^{-1}(T) = -\frac{1}{2a} + \frac{1}{2a}\left(1 - 8a + 4ae^T\right)^{1/2}$$

et on trouve

$$\lambda^{-1}(p\lambda(T)) = f(T).$$

Le groupe formel $F(X,Y)$ est donc le groupe $F_f(X,Y)$ et on a bien l'équivalence $(i) \Leftrightarrow (ii)$.
Les endomorphismes du groupe $F_f(X,Y)$ étant les séries $\lambda^{-1}(\alpha\lambda(T))$, on obtient :

$$\sigma^f_{\alpha^{-1}}(T) = [\alpha]_{ff}(T) = \frac{1}{a}\left(a(1+T+aT^2)^{\alpha} + \frac{1}{4} - a\right)^{1/2} - \frac{1}{2}a.$$

Soient α_1,...,$\alpha_n \in U_p$, par le théorème 2.5.1, on obtient les équivalences suivantes :

(i) Les nombres 1, α_1, α_2,...,α_n sont $\mathbb{Z}$-linéairement indépendants,

(ii) Les séries $\widetilde{\sigma}^f_{\alpha_1}(T)$,..., $\widetilde{\sigma}^f_{\alpha_n}(T)$ sont algébriquement indépendantes sur $\mathbb{F}_p(T)$.

Théorème 2.5.2 *Soit une série $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ telle que sa projection dans $\mathbb{F}_p[[T]]$ soit algébrique sur $\mathbb{F}_p(T)$ et soit $\lambda(T) = \log(1+\gamma(T))$.*
Soient $\lambda_1, ..., \lambda_n \in U_p$. Si l'on pose

$$f(T) = \lambda^{-1}(p\lambda(T)) \in \mathcal{F}_p,$$

les assertions suivantes sont équivalentes :

(i) *Les éléments 1, λ_1,...,λ_n sont $\mathbb{Z}$-linéairement indépendants,*

(ii) *Les séries $\widetilde{\sigma}^f_{\lambda_i,2}(T)$, $i = 1, ..., n$ sont algébriquement indépendantes sur $\mathbb{F}_p(T)$.*

Preuve : Nous avons vu au paragraphe 2.4.2 que les endomorphismes réduits $\widetilde{\sigma}^f_{\lambda_i,2}(T)$ sont en fait les restrictions des automorphismes du corps de normes Y_f d'une extension A.P.F. de $\mathbb{Q}_p$ à son sous-corps $X_f^{(2)}$. Il a été prouvé dans ce cas, au paragraphe 2.4.4, que si l'on note T une uniformisante de Y_f, alors la série $\pi(T) = N_{Y_f/X_f^{(2)}}(T)$ est algébrique sur $\mathbb{F}_p(T)$.
De plus, nous avons la relation :

$$\pi \circ \widetilde{\sigma}^f_{\lambda_i}(T) = \widetilde{\sigma}^f_{\lambda_i,2} \circ \pi(T) \text{ pour } i = 1, ..., n.$$

La série $\pi(T)$ étant algébrique sur $\mathbb{F}_p(T)$, les séries $\widetilde{\sigma}^f_{\lambda_i}(T)$ sont algébriquement indépendantes si et seulement si les séries $\widetilde{\sigma}^f_{\lambda_i,2}(T)$ le sont.
On conclut à l'équivalence voulue en utilisant le théorème 2.5.1.

2.5.3 Indépendance algébrique des "séries" de Chebyshev

Théorème 2.5.3 *Soient $\lambda_1, ..., \lambda_n \in U_p$ et soit $S_{\lambda_i}(T)$ la série de Chebyshev associée à λ_i pour $i = 1, ..., n$. Les assertions suivantes sont équivalentes :*

(i) *Les éléments 1, λ_1,...,λ_n sont $\mathbb{Z}$-linéairement indépendants,*

(ii) *Les séries $\widetilde{S}_{\lambda_i}(T)$, $i = 1, ..., n$ sont algébriquement indépendantes sur $\mathbb{F}_p(T)$.*

Preuve : L'équivalence est établie dans le théorème 2.5.2 dans le cas des séries $\widetilde{\sigma}^f_{\lambda_i,2}(T)$ avec $f(T) = (1+T)^p - 1$. Comme on a la relation

$$S_{\lambda_i}(T) = 1 - \frac{1}{2}\sigma^f_{\lambda_i,2}(2 - T),$$

on obtient le résultat voulu.
Remarque : Nous avons vu au lemme 2.1.8 que pour $f(T) = 3T + T^3$, les séries $\widetilde{\sigma}^f_\lambda(T)$ pour $\lambda \in U_3$ sont les séries

$$\left(\frac{T + (4 + T^2)^{1/2}}{2}\right)^\lambda - \left(\frac{T + (4 + T^2)^{1/2}}{2}\right)^{-\lambda} \bmod 3.$$

Comme on sait qu'il existe des isomorphismes entre le groupe multiplicatif et le groupe de Lubin-Tate sur $\mathbb{Z}_3$ défini par $f(T)$ qui sont de réduction modulo 3 algébrique sur $\mathbb{F}_3(T)$, on peut alors affirmer que les assertions suivantes sont équivalentes :

- Les unités 3-adiques 1, λ_1,...,λ_n sont $\mathbb{Z}$-linéairement indépendantes,
- La famille constituée des séries $\left(\frac{T + (4 + T^2)^{1/2}}{2}\right)^{\lambda_i} - \left(\frac{T + (4 + T^2)^{1/2}}{2}\right)^{-\lambda_i} \bmod 3$ est algébriquement indépendante sur $\mathbb{F}_3(T)$.

2.6 Résultats de transcendance sur les séries d'Artin-Hasse

2.6.1 Le logarithme

Le logarithme d'Artin-Hasse $l(1 + T)$ a pour expression :

$$l(1 + T) = \log\left(\frac{1 + T}{(1 + T^p)^{1/p}}\right).$$

Le calcul nous montre alors que

$$l(1 + T) = \sum_{i=1}^{+\infty} (-1)^{i-1}\delta_i \frac{T^i}{i}$$

avec $\delta_i = 1$ si p ne divise pas i
$= 0$ sinon.

On a $l(1+T) \in \mathbb{Z}_p[[T]]$ et si l'on écrit $l(1+T) = \sum_{i \geq 1} \alpha_i T^i$, on vérifie aisément que pour tout $k \in \mathbb{N}$, $\alpha_k \equiv \alpha_{k+2p} \pmod{p}$. D'où la proposition :

Proposition 2.6.1 *La projection $\widetilde{l}(1+T)$ de $l(1+T)$ sur $\mathbb{F}_p[[T]]$ est une série rationelle sur $\mathbb{F}_p$.*

Posons $L(T) = l(1+T)$. Soit $L^{-1}(T)$ l'inverse de composition de la série $L(T)$ et soit $f(T) = L^{-1}((1+L(T))^p - 1) \in \mathcal{F}_p$.

Corollaire 2.6.1 *Soit $\alpha \in U_p$. Les assertions suivantes sont équivalentes :*

(i) $\alpha \in \mathbb{Q}$,

(ii) *La série $\widetilde{\sigma}_\alpha^f(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : Comme $L(T) \in \mathbb{Z}_p[[T]]$ vérifie $L(T) \equiv T \pmod{\deg 2}$ avec $\widetilde{L}(T)$ algébrique (car rationnelle) sur $\mathbb{F}_p(T)$, on applique le théorème 2.1.3 avec $\gamma(T) = L(T)$ et les $\sigma_\alpha^f(T)$ sont les endomorphismes du groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ admettant pour logarithme la série

$$\lambda(T) = \log\left(1 + \log(1+T) - \frac{1}{p}\log(1+T^p)\right) \in \mathbb{Q}_p[[T]].$$

Remarque : Soient $\alpha_1,...,\alpha_n \in U_p$. En appliquant le théorème 2.5.1, on obtient les assertions équivalentes :

(i) Les nombres p-adiques 1, α_1, α_2,..., α_n sont $\mathbb{Z}$-linéairement indépendants,

(ii) Les séries $\widetilde{\sigma}_{\alpha_1}^f(T)$,..., $\widetilde{\sigma}_{\alpha_n}^f(T)$ sont algébriquement indépendantes sur $\mathbb{F}_p(T)$.

2.6.2 L'exponentielle

On note $E(T)$ l'exponentielle d'Artin-Hasse définie par $E(T) = exp\left(\sum_{i=0}^{+\infty} \frac{T^{p^i}}{p^i}\right)$. On a le théorème :

Théorème 2.6.1 *Soit $\gamma(T) \in T + T^2\mathbb{Z}_p[[T]]$ et soit*

$$g(T) = \log\left(\frac{1+\gamma(T)}{(1+\gamma(T^p))^{1/p}}\right) = \sum_{i=1}^{+\infty} b_i T^i.$$

Les assertions suivantes sont équivalentes :

(i) *La série $\gamma(T)$ réduite modulo p est algébrique sur $\mathbb{F}_p(T)$,*

(ii) *La série* $\prod_{i=1}^{+\infty} E(T^i)^{b_i}$ *réduite modulo p est algébrique sur* $\mathbb{F}_p(T)$.

Preuve : La série $\gamma(T)$ est un isomorphisme entre le groupe multiplicatif et le groupe de logarithme $\log(1+\gamma(T))$. Comme $\gamma(T) \equiv T \pmod{\deg 2}$, d'après le corollaire 2.1.1, la série $\prod_{i=1}^{+\infty} E(T^i)^{b_i} - 1$ est ce même isomorphisme, d'où la conclusion.

Corollaire 2.6.2 *Soit p un nombre premier. Considérons la suite* $(b_n)_n$ *d'éléments de* $\mathbb{Z}_p$ *définie par*

$$\begin{aligned} b_n &= \frac{1}{n} \text{ si } p \text{ ne divise pas } n \\ &= 0 \text{ sinon.} \end{aligned}$$

Alors la série $\prod_{n=1}^{+\infty} E(T^n)^{b_n}$ *réduite modulo p est algébrique sur* $\mathbb{F}_p(T)$.

Preuve : La série $g(T) = \sum_{n=1}^{+\infty} b_n T^n$ est en fait la série logarithmique d'Artin-Hasse :

$$g(T) = l(1+T) = \log\left(\frac{1+T}{(1+T^p)^{1/p}}\right).$$

Cela signifie que $\gamma(T) = T$, d'où la conclusion.

2.7 Automorphismes algébriques avec $car(K) = p$

2.7.1 Notations

Soit p un nombre premier supérieur ou égal à 3. Soit le corps local $K = \mathbb{F}_p((t))$ de caractéritique p muni de sa valuation t-adique. On prend $A = \mathbb{F}_p[[t]]$, $U = \mathbb{F}_p[[t]]^*$ (groupe multiplicatif des éléments inversibles de A) et $\pi = t$. On munit U de sa filtration : $U^{(n)} = 1 + t^n A$ pour tout $n \in \mathbb{N}$.
On pose

$$\mathcal{F}_t = \{f(T) \in A[[T]] | f(T) \equiv tT \pmod{\deg 2},\ f(T) \equiv T^p \pmod{t}\}$$

et on définit comme précédemment le groupe $\widetilde{\mathcal{F}} = \{f(T) \in \mathbb{F}_p[[T]] | v_T(f) = 1\}$ muni de la loi de composition.
Pour $f(T) \in \mathcal{F}_t$ et d diviseur de $p-1$, on définit L, L_∞, G, $\mathcal{T}$, $\mathcal{T}^{(d)}$, $K_\infty^{(d)}$, Y_f, $X_f^{(d)}$, σ_u^f et $\sigma_{u,d}^f$ comme en 2.2.1 et 2.2.2.
On a $G \simeq \mu_{p-1} \times \mathbb{Z}_p^\infty$, $\mathcal{T} \simeq \mu_{p-1}$ et $\mathcal{T}^{(d)} \simeq \mu_d$.
Soit $f(T) = tT + T^p \in \mathcal{F}_t$ et $F_f(X,Y)$ l'unique groupe formel de Lubin-Tate admettant

$f(T)$ pour endomorphisme. Pour tout $u^{-1} = \sum_{i=0}^{\infty} \alpha_i t^i \in U$, le calcul montre que $\widetilde{\sigma}_u^f(T) = \sum_{i=0}^{\infty} \alpha_i T^{p^i} \in \mathbb{F}_p[[T]]$ (voir [35]). Soit $\mathcal{G} = \{\widetilde{\sigma}_u^f(T) | u \in U\}$ muni de la loi de composition. Alors $\mathcal{G}$ est un sous-groupe de $\mathrm{Aut}(Y)$ isomorphe en tant que groupe filtré à U.

2.7.2 Caractérisation de la série $\widetilde{\sigma}_{u,d}^f(T)$

Soient δ un générateur de $\mathbb{F}_p^*$,

$$\Gamma = \{\delta^i T | i = 0, 1, ..., p-2\}$$

et

$$\Gamma^{(d)} = \{\delta^{i\frac{p-1}{d}} T | i = 0, 1, ..., d-1\}$$

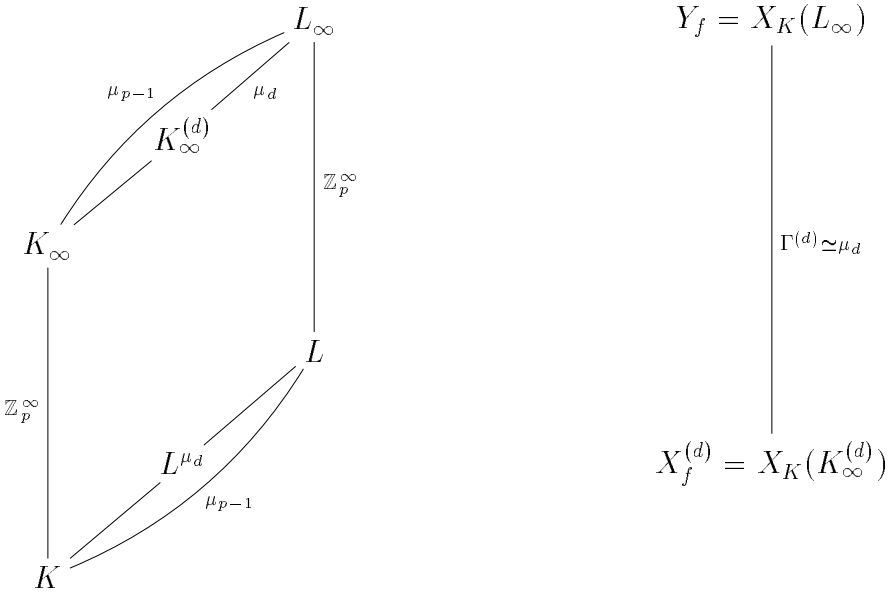
munis de la composition.

Lemme 2.7.1 *Le quotient $\mathcal{G}/\mathcal{G}_{p-1}$ est isomorphe à Γ où $\mathcal{G}_{p-1} = \{g(T) \in \mathcal{G} | i_T(g) \geq p-1\}$.*

Preuve : Soit $\widetilde{\sigma}_u^f(T) = \sum_{i=0}^{\infty} \alpha_i T^{p^i}$, alors $\widetilde{\sigma}_u^f(T) \equiv \alpha_0 T \pmod{\mathcal{G}_{p-1}}$. D'où la conclusion.

Lemme 2.7.2 *Le groupe de Galois de l'extension $Y_f/X_f^{(d)}$ est $Gal(Y_f/X_f^{(d)}) = \Gamma^{(d)}$.*

Preuve : Comme $Gal(L_\infty/K_\infty)$ est isomorphe à $U/U^{(1)}$, $Gal(Y_f/X_f)$ est isomorphe à $\mathcal{G}/\mathcal{G}^1 = \mathcal{G}/\mathcal{G}_{\Psi(1)} = \mathcal{G}/\mathcal{G}_{p-1}$. Donc, d'après le lemme 2.7.1, $Gal(Y_f/X_f)$ est isomorphe à Γ.
Γ étant le seul sous-groupe de $\mathcal{G}$ d'ordre $p-1$, on peut en déduire que $Gal(Y_f/X_f) = \Gamma$.
Le groupe $Gal(Y_f/X_f^{(d)})$ est l'unique sous-groupe de Γ d'ordre d; il s'agit de $\Gamma^{(d)}$.



Lemme 2.7.3 *Si l'on pose* $Y_f = \mathbb{F}_p((T))$, *alors* $X_f^{(d)}$ *est le corps* $\mathbb{F}_p((\theta_d))$ *avec* $\theta_d = (-1)^{d+1}T^d$ *pour* d *diviseur de* $p-1$.

Preuve : Il suffit de remarquer que $\theta_d(T) = N_{Y_f/X_f^{(d)}}(T)$.

Proposition 2.7.1 *Soit* $\widetilde{\Delta}_u^{(d)}(T) = N_{Y_f/X_f^{(d)}}(\widetilde{\sigma}_u^f(T))$. *Alors on a la relation suivante :*

$$\widetilde{\Delta}_1^{(d)}(\widetilde{\sigma}_u^f(T)) = \widetilde{\sigma}_{u,d}^f(\widetilde{\Delta}_1^{(d)}(T)).$$

Remarque : Pour u et v éléments de U on a :

$$\widetilde{\sigma}_{uv,d}^f(T) = \widetilde{\sigma}_{vu,d}^f(T) = \widetilde{\sigma}_{u,d}^f \circ \widetilde{\sigma}_{v,d}^f(T) = \widetilde{\sigma}_{v,d}^f \circ \widetilde{\sigma}_{u,d}^f(T).$$

2.7.3 Calcul de la série $\widetilde{\sigma}_{u,d}^f(T)$

Calculs effectifs de $\widetilde{\sigma}_{u,d}^f(T)$

On rappelle que l'on note $B_{n,k}$ les polynômes de Bell du paragraphe 2.3.

Théorème 2.7.1 *Soit* $u(t) \in \mathbb{F}_p[[t]]^*$ *tel que son inverse multiplicatif* $u^{-1}(t)$ *s'écrive* $u^{-1} = \sum_{i=0}^{+\infty} u_i t^i \in \mathbb{F}_p[[t]]^*$ *et soit la suite* $(x_n)_{n\geq 1} \in \mathbb{F}_p^{\mathbb{N}}$ *définie par*

$$\begin{aligned} x_n &= n!u_k \text{ si } n = p^k \\ &= 0 \text{ si } n \text{ n'est pas une puissance de } p. \end{aligned}$$

Soit $d \geq 2$ *un diviseur de* $p-1$ *et soit*

$$\widehat{B}_{n,d} = (-1)^{(d+1)(n+1)} \frac{B_{nd,d}(x_1, x_2, \ldots x_{nd-d+1})d!}{(nd)!} \bmod p.$$

Alors :

$$\widetilde{\sigma}_{u,d}^f(T) = \sum_{n\geq 1} \widehat{B}_{n,d} T^n.$$

Preuve : On va voir que la réduction modulaire est bien définie, par construction de l'élément $\widehat{B}_{n,d}$.
On part de l'égalité :

$$\widetilde{\Delta}_1^{(d)}(\widetilde{\sigma}_u^f(T)) = \widetilde{\sigma}_{u,d}^f(\widetilde{\Delta}_1^{(d)}(T)).$$

Il vient alors : $\widetilde{\Delta}_1^{(d)}(\widetilde{\sigma}_u^f(T)) = (-1)^{d+1}\widetilde{\sigma}_u^f(T)^d = (-1)^{d+1}\left(\sum_{i=0}^{+\infty} u_i T^{p^i}\right)^d$. Cette série est de manière évidente à coefficients dans $\mathbb{F}_p$. Avec les notations du théorème, nous pouvons écrire qu'elle est égale à

$$(-1)^{d+1}\left(\sum_{n=1}^{+\infty} \frac{x_n}{n!} T^n\right)^d$$

qui est donc aussi une série à coefficients dans $\mathbb{F}_p$.
L'écriture en fonction des x_n nous permet maintenant d'utiliser les polynômes de Bell. On obtient :

$$(-1)^{d+1}\widetilde{\sigma}_u^f(T)^d = d!\left(\sum_{n\geq d}(-1)^{d+1}\frac{B_{n,d}}{n!}T^n\right) = (A)$$

toujours avec des séries à coefficients dans $\mathbb{F}_p$. Or la série (A) est en fait une série en $(-1)^{d+1}T^d$. D'où :

$$(A) = \left(d!\sum_{n\geq d}(-1)^{(d+1)(\frac{n}{d}+1)}\frac{B_{n,d}}{n!}T^{\frac{n}{d}}\right)\circ((-1)^{d+1}T^d).$$

La notation $T^{n/d}$ a un sens car la série $\widetilde{\sigma}_{u,d}^f(T)$ étant $\mathbb{F}_p[[T]]$, pour tout d ne divisant pas n, on a $B_{n,d} = 0$. Ainsi $\widetilde{\sigma}_{u,d}^f(T)$ est la projection de la série

$$d!\sum_{n\geq d}(-1)^{(d+1)(\frac{n}{d}+1)}\frac{B_{n,d}}{n!}T^{\frac{n}{d}}$$

dans $\mathbb{F}_p[[T]]$. Par changement de variable, on obtient alors

$$\widetilde{\sigma}_{u,d}^f(T) = \sum_{n\geq 1}\left((-1)^{(d+1)(n+1)}\frac{d!}{(nd)!}B_{nd,d} \bmod p\right)T^n.$$

Remarque : Si $d = p-1$ alors $\widehat{B}_{n,p-1} = (-1)^{(n+1)}\dfrac{B_{n(p-1),p-1}}{n!} \bmod p$.

Le cas $p = 3$

Dans le cas où $p = 3$, les coefficients de $\widetilde{\sigma}_{u,2}^f(T)$ peuvent être calculés par la récurrence suivante :
Soit $u^{-1} = \sum_{i=0}^{+\infty} u_i t^i \in \mathbb{F}_3[[t]]$. Alors $\widetilde{\sigma}_{u,2}^f(T) = \sum_{i=0}^{+\infty}\alpha_i T^{a_i} \in \mathbb{F}_3[[T]]$ avec :

$$\begin{aligned}
a_0 &= 2 = 3^0 + 3^0,\\
a_{i+1} &= 3^{n+1} + 3^0 \text{ si } a_i \text{ est de la forme } 3^n + 3^n,\\
&= 3^n + 3^{k+1} \text{ si } a_i \text{ est de la forme } 3^n + 3^k \text{ avec } 0 \leq k \leq n-1,\\
\alpha_0 &= (-1)^{\frac{a_0}{2}+1}u_0^2,\\
\alpha_{i+1} &= 2(-1)^{\frac{a_{i+1}}{2}+1}u_0u_{n+1} \text{ si } \alpha_i \text{ est de la forme } (-1)^{\frac{a_i}{2}+1}u_n^2,\\
&= 2(-1)^{\frac{a_{i+1}}{2}+1}u_{k+1}u_n \text{ si } \alpha_i \text{ est de la forme } 2(-1)^{\frac{a_i}{2}+1}u_ku_n \text{ où } 0 \leq k \leq n-2,\\
&= (-1)^{\frac{a_{i+1}}{2}+1}u_n^2 \text{ si } \alpha_i \text{ est de la forme } 2(-1)^{\frac{a_i}{2}+1}u_{n-1}u_n.
\end{aligned}$$

Exemples numériques

$p = 3$ et $d = 2$

u^{-1}	$\widetilde{\sigma}_u^f(T)$	$\widetilde{\sigma}_{u,2}^f(T)$
$1+t$	$T+T^3$	$T+T^2+T^3$
$2+t^2$	$2T+T^9$	$T+T^5+T^9$
$1+t+t^2$	$T+T^3+T^9$	$T+T^2+T^3+2T^5+T^6+T^9$
$2+t^4$	$2T+T^{81}$	$T+T^{41}+T^{81}$

$p = 7$ et $d = 2$

u^{-1}	$\widetilde{\sigma}_u^f(T)$	$\widetilde{\sigma}_{u,2}^f(T)$
$3+t+t^7$	$3T+T^7+T^{823543}$	$2T+T^4+T^7+T^{411772}+2T^{411775}+T^{823543}$
$1+t^9$	$T+T^{40353607}$	$T+5T^{20176804}+T^{40353607}$
$1+t$	$T+T^7$	$T+5T^4+T^7$

$p = 7$ et $d = 3$

u^{-1}	$\widetilde{\sigma}_u^f(T)$	$\widetilde{\sigma}_{u,3}^f(T)$
$1+t^9$	$T+T^{40353607}$	$T+3T^{13451203}+3T^{26902405}+T^{40353607}$
$1+t$	$T+T^7$	$T+3T^3+3T^5+T^7$

2.7.4 Algébricité des automorphismes et des restrictions

Théorème 2.7.2 *Soit $u \in U = \mathbb{F}_p[[t]]^*$ et soit $d \geq 2$ un diviseur de $p-1$. Alors les assertions suivantes sont équivalentes :*

(i) $u \in \mathbb{F}_p(t)$,

(ii) *La série $\widetilde{\sigma}_u^f(T)$ est algébrique sur $\mathbb{F}_p(T)$,*

(iii) *La série $\widetilde{\sigma}_{u,d}^f(T)$ est algébrique sur $\mathbb{F}_p(T)$.*

Preuve : Nous admettons pour l'instant le résultat suivant (conjecturé par F. Laubie et démontré par J.-P. Allouche [2]) :

Soit $(u_i)_{i\geq 0}$ une suite à coefficients dans $\mathbb{F}_p$. Alors la série $\displaystyle\sum_{i=0}^{+\infty} u_i T^{p^i}$ est algébrique sur $\mathbb{F}_p(T)$ si et seulement si la suite $(u_i)_{i\geq 0}$ est ultimement périodique. La preuve de cette équivalence sera donnée au chapitre 3.
Pour établir $(ii) \Leftrightarrow (iii)$, on utilise le fait que la norme de Y_f à $X_f^{(d)}$ de T est égale à $(-1)^{d-1}T^d$, c'est-à-dire algébrique sur $\mathbb{F}_p(T)$. On obtient le résultat voulu en appliquant la proposition 2.2.4.

Interprétation p-automatique

Théorème 2.7.3 *Soit $u^{-1} = \displaystyle\sum_{i=0}^{+\infty} u_i t^i \in \mathbb{F}_p[[t]]^*$ et soit la suite $(x_n)_{n\geq 1} \in \mathbb{F}_p^{\mathbb{N}}$ définie par*

$$\begin{aligned} x_n &= n! u_k \text{ si } n = p^k \\ &= 0 \text{ si } n \text{ n'est pas une puissance de } p. \end{aligned}$$

Soit $d \geq 2$ un diviseur de $p-1$ et $\widehat{B}_{n,d} = (-1)^{(d+1)(n+1)} \dfrac{B_{nd,d}\, d!}{(nd)!} \bmod p$. Alors les assertions suivantes sont équivalentes :

(i) $u \in \mathbb{F}_p(t)$,

(ii) *La suite $(\widehat{B}_{n,d})_{n\geq 1}$ est p-automatique.*

2.7.5 Une conséquence de la ramification

Théorème 2.7.4 *Soit $d \geq 2$ un diviseur de $p-1$ et soit $M = Max\{v_t(\delta u - 1) | \delta \in \mu_d\}$. Alors pour tout $u \in U$ on a :*

$$v_T\left(\frac{\widetilde{\sigma}^f_{u,d}(T)}{T} - 1\right) = \frac{1}{d}(p^M - 1).$$

Preuve : On sait que U et $\mathcal{G}$ sont isomorphes en tant que groupes filtrés [31, 35]. Si l'on pose

$$i_t(u) = v_t(u-1)$$

et

$$i_T(g(T)) = v_T\left(\frac{g(T)}{T} - 1\right),$$

les fonctions d'ordre de la filtration en numérotation supérieure de U et $\mathcal{G}$ sont respectivement :

$$u \longmapsto i_t(u)$$
$$\widetilde{\sigma}^f_u(T) \longmapsto \Phi_{\mathcal{G}}(i_T(\widetilde{\sigma}^f_u(T)))$$

où $\Phi_{\mathcal{G}}$ est la fonction réciproque de la fonction $\Psi_{\mathcal{G}}$ de Herbrand relative à $\mathcal{G}$.
Ainsi

$$U^{(\alpha)} = \{u \in U | i_t(u) \geq \alpha\}$$

et

$$\begin{aligned} \mathcal{G}^\alpha &= \left\{\widetilde{\sigma}^f_u(T) \in \mathcal{G} \,|\, \Phi_{\mathcal{G}}(i_T(\widetilde{\sigma}^f_u(T))) \geq \alpha\right\} \\ &= \left\{\widetilde{\sigma}^f_u(T) \in \mathcal{G} \,|\, i_T(\sigma^f_u(T)) \geq \Psi_{\mathcal{G}}(\alpha)\right\}. \end{aligned}$$

Par la suite, on notera H_d le sous-groupe de U isomorphe à μ_d et $\mathcal{H}_d$ son image dans $\mathcal{G}$.
Le groupe $\mathcal{G}/\mathcal{H}_d$ s'identifie à un sous-groupe de $\mathrm{Aut}(X_f^{(d)})$ isomorphe en tant que groupe filtré à U/H_d. Par la théorie de Galois, $\mathcal{G}/\mathcal{H}_d$ est le groupe des restrictions des éléments de $\mathcal{G}$ à $X^{(d)}$. Pour $\alpha \geq 0$, on a

$$(\mathcal{G}/\mathcal{H}_d)^\alpha \simeq (U/H_d)^\alpha.$$

Il vient :

$$\begin{aligned} (\mathcal{G}/\mathcal{H}_d)^\alpha &= \left\{\overline{\widetilde{\sigma}^f_u} \in \mathcal{G}/\mathcal{H}_d \,|\, \Phi_{\mathcal{G}/\mathcal{H}_d}(Max_{\delta\in H_d}\{i_T(\widetilde{\sigma}^f_u \circ \mu_\delta)\}) \geq \alpha\right\} \\ &= \left\{\overline{\widetilde{\sigma}^f_u} \in \mathcal{G}/\mathcal{H}_d \,|\, Max_{\delta\in H_d}\{\Phi_{\mathcal{G}/\mathcal{H}_d}(i_T(\widetilde{\sigma}^f_u \circ \mu_\delta))\} \geq \alpha\right\}. \end{aligned}$$

D'où

$$\begin{aligned}(U/H_d)^{\alpha} &= \{\overline{u} \in U/H_d | Max_{\delta \in H_d}\{i_t(u\delta)\} \geq \alpha\} \\ &= \{\overline{u} \in U/H_d | Max_{\delta \in H_d}\{v_t(u\delta - 1)\} \geq \alpha\}\,.\end{aligned}$$

On peut alors écrire :

$$\begin{aligned}v_T\left(\frac{\widetilde{\sigma}^f_{u,d}(T)}{T} - 1\right) \geq \alpha \quad &\Leftrightarrow \quad i_T(\widetilde{\sigma}^f_{u,d}(T)) \geq \alpha \\ &\Leftrightarrow \quad \widetilde{\sigma}^f_{u,d} \in (\mathcal{G}/\mathcal{H}_d)_{\alpha} \\ &\Leftrightarrow \quad \widetilde{\sigma}^f_{u,d} \in (\mathcal{G}/\mathcal{H}_d)^{\Phi_{\mathcal{G}/\mathcal{H}_d}(\alpha)} \\ &\Leftrightarrow \quad \overline{u} \in (U/H_d)^{\Phi_{U/H_d}(\alpha)} \\ &\Leftrightarrow \quad Max_{\delta \in H_d}\{v_t(u\delta - 1)\} \geq \Phi_{U/H_d}(\alpha) \\ &\Leftrightarrow \quad \Psi_{U/H_d}(Max_{\delta \in H_d}\{v_t(u\delta - 1)\}) \geq \alpha.\end{aligned}$$

Calculons $\Psi_{U/H_d}(x)$:
On sait que $\Psi_U = \Psi_{H_d} \circ \Psi_{U/H_d}$ [35]. De plus

$$\Psi_{H_d}(x) = \int_0^x (H_d : H_d^s) ds$$

avec $(H_d : H_d^0) = 1$ et $(H_d : H_d^s) = d$ si $s > 0$. D'où $\Psi_{H_d}(x) = dx$. Ainsi

$$\Psi_{U/H_d}(x) = \frac{1}{d}\Psi_U(x).$$

Or on sait que $\Psi_U(m) = p^m - 1$ si m est entier. On en déduit que pour tout entier m :

$$\Psi_{U/H_d}(m) = \frac{1}{d}(p^m - 1).$$

Comme $Max_{\delta \in H_d}\{v_t(u\delta - 1)\}$ est une valeur entière, on obtient l'égalité voulue.

Corollaire 2.7.1 *Soit $u \in U^{(n)}$ et soit $k = \frac{1}{d}(p^n - 1)$. Alors les puissances de T dans $\widetilde{\sigma}^f_{u,d}(T)$ comprises entre 2 et k ont leur coefficient nul. Le monôme de degré $k+1$ a quant à lui un coefficient non nul. En d'autres termes :*

$$u \in U^{(n)} \Longrightarrow \widetilde{\sigma}^f_{u,d}(T) \equiv T + \alpha_{k+1}T^{k+1} \pmod{\deg k + 2}$$

avec $\alpha_{k+1} \neq 0$.

Preuve : Si $u \in U^{(n)}$ alors $u = 1 + \alpha_n t^n + \alpha_{n+1}t^{n+1} + ...$
Pour $\delta \in \mu_d$,

$$\begin{aligned}v_t(u\delta - 1) &= 0 \text{ si } \delta \neq 1 \\ &= n \text{ si } \delta = 1.\end{aligned}$$

D'où $M = n$ ce qui prouve le corollaire.

Corollaire 2.7.2 *Soient $u \in U^{(n)}$ et $(x_n)_{n\in\mathbb{N}}$ définie comme au théorème 2.7.3. On pose*

$$k = \frac{1}{d}(p^n - 1).$$

Alors :

(i) $\widehat{B}_{1,d} = 1$

(ii) $\widehat{B}_{n,d} = 0$ *si* $2 \leq n \leq k$

(iii) $\widehat{B}_{(k+1),d} \neq 0$

Preuve : C'est évident à partir de l'écriture des $\widetilde{\sigma}^f_{u,d}(T)$.

Corollaire 2.7.3 *Soit $u \in U$ tel que $u \notin U^{(1)}$. Soient $\eta = u^{-1} \bmod \deg 1$, $n = v_t(u^{-1} - \eta)$ et $k = \frac{1}{d}(p^n - 1)$. Alors, si $\eta \in \mu_d$ on a :*

(i) $\widehat{B}_{1,d} = \eta$

(ii) $\widehat{B}_{n,d} = 0$ *si* $2 \leq n \leq k$

(iii) $\widehat{B}_{(k+1),d} \neq 0$

Preuve : Si $\eta \in \mu_d$, alors il existe $\eta' \in \mu_d$ tel que $\eta\eta' = 1$ et dans ce cas, $M = n$.

Chapitre 3

Modules de Drinfeld et automates

Nous nous proposons d'établir, dans cette partie, un analogue du théorème 2.1.3 dans le cas où l'on remplace l'anneau $\mathbb{Z}_p$ par le complété $P(t)$-adique de l'anneau $\mathbb{F}_q[t]$ où $P(t) \in \mathbb{F}_q[t]$ est irréductible et unitaire.

3.1 Modules de Drinfeld, module de Carlitz

Soit K un corps de caractéristique p et soit q une puissance d'un nombre premier p. On définit le morphisme σ par :

$$\begin{array}{rcl} \sigma & : & K \to K \\ & & x \mapsto x^q \end{array}$$

Si $K = \mathbb{F}_q(t)$, le morphisme σ est l'endomorphisme de Frobenius.
On note $K\{\sigma\}$ l'anneau des polynômes de Ore, c'est-à-dire l'anneau des polynômes

$$a_0 id + a_1\sigma^1 + ... + a_n\sigma^n$$

muni de l'addition et de la multiplication de Ore. On représente par $K\{\{\sigma\}\}$ l'anneau des séries de Ore que l'on peut voir comme étant l'anneau des séries

$$\sum_{i=0}^{+\infty} a_i T^{q^i}$$

muni de l'addition et de l'opération de composition en caractéristique p.

Définition 3.1.1 *Soit $\mathcal{A}$ un anneau intègre qui est une $\mathbb{F}_q$-algèbre et soit K un sur-corps commutatif de $\mathbb{F}_q$. On dit que K est un $\mathcal{A}$-corps s'il existe un morphisme de $\mathbb{F}_q$-algèbres $i : \mathcal{A} \to K$. Le morphisme i s'appelle le morphisme structural de K.*

Définition 3.1.2 Application D :
Soit $f(\sigma) = a_0\sigma^0 + a_1\sigma^1 + ... + a_n\sigma^n \in K\{\sigma\}$. On définit l'application D par :

$$\begin{array}{rcl} D & : & K\{\sigma\} \to K \\ & & f(\sigma) \mapsto D(f) = a_0 \end{array}$$

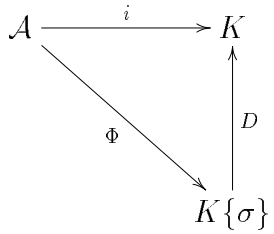
Définition 3.1.3 *Soit $\mathcal{A}$ un anneau intègre qui est une $\mathbb{F}_q$-algèbre et soit K un $\mathcal{A}$-corps de morphisme structural i. Soit une application Φ :*

$$\begin{array}{rcl} \Phi & : & \mathcal{A} \to K\{\sigma\} \\ & & P \mapsto \Phi_P \end{array}$$

qui est un morphisme de $\mathbb{F}_q$-algèbre. On dit que Φ est un module de Drinfeld sur K si :

(i) $D \circ \Phi = i$

(ii) *Le morphisme Φ n'est pas trivial.*



Remarque : Si $\mathcal{A} = \mathbb{F}_q[t]$, l'application $P \mapsto \Phi_P$ étant un morphisme de $\mathbb{F}_q$-algèbre, la donnée de Φ_t suffit à déterminer complètement le module de Drinfeld Φ.

On suppose dorénavant que l'anneau $\mathcal{A}$ contient $\mathbb{F}_q[t]$ et est tel que tout module de Drinfeld Φ sur un $\mathcal{A}$-corps K est complètement déterminé par la donnée de Φ_t.

Définition 3.1.4 *On définit le module de Carlitz comme étant le module de Drinfeld sur un $\mathcal{A}$-corps K caractérisé par*

$$\Phi_t = \gamma_t = t\sigma^0 + \sigma$$

que l'on peut noter en considérant son action sur un paramètre formel T :

$$\gamma_t(T) = tT + T^q.$$

Par la suite, T désignera un élément transcendant sur $\mathbb{F}_q(t)$.

Définition 3.1.5 *Soient Φ et Φ' deux modules de Drinfeld sur un $\mathcal{A}$-corps K. Une isogénie de Φ sur Φ' est un polynôme $Q \in K\{\sigma\}$, non nul, tel que pour tout $P \in \mathcal{A}$:*

$$Q\Phi_P = \Phi'_P Q.$$

On dit que deux modules de Drinfeld sont isomorphes sur un corps L si $Q = \alpha\sigma^0$ avec $\alpha \in L$. On dit dans ce cas que l'isogénie Q est un isomorphisme de modules de Drinfeld.

Définition 3.1.6 *On appelle rang d'un module de Drinfeld le "degré" en σ de Φ_t.*

Remarque : Le module de Carlitz est donc de rang 1.

Définition 3.1.7 *On définit l'ensemble $End_K\Phi$ des endomorphismes du module de Drinfeld Φ sur le $\mathcal{A}$-corps K par*

$$End_K(\Phi) = \{Q \in K\{\sigma\}, Q\Phi_P = \Phi_P Q, \forall P \in \mathcal{A}\}$$

Nous allons donner maintenant la définition des dérivées galoisiennes introduites par Y. Hellgouarch dans [22] afin d'obtenir des calculs explicites sur les endomorphismes du module de Carlitz.

Définition 3.1.8 *Soit x appartenant à un $\mathcal{A}$-corps K. On définit les dérivées galoisiennes $D^{(i)}(x) \in K$ par la formule de récurrence :*

$$\begin{aligned} D^{(0)}(x) &= x \\ D^{(i)}(x) &= \frac{\left(D^{(i-1)}(x)\right)^q - D^{(i-1)}(x)}{t^{q^i} - t} \end{aligned}$$

Théorème 3.1.1 (Hellegouarch [22])
Soit $\mathcal{A} = \mathbb{F}_q[t]$ et soit $P(t) \in \mathcal{A}$ de degré n. On a :

$$\gamma_P(T) = \sum_{i=0}^{n} D^{(i)}(P)\sigma^i(T) = \sum_{i=0}^{n} D^{(i)}(P)T^{q^i}.$$

Proposition 3.1.1 (Hellegouarch [22]) *Les dérivées galoisiennes vérifient la formule de Leibniz :*
Pour tous x et y dans K et $n \geq 0$:

$$D^{(n)}(xy) = \sum_{i=0}^{n} D^{(i)}(x)\left(D^{(n-i)}(y)\right)^{q^i}.$$

3.2 Modules de Drinfeld formels

Définition 3.2.1 L'exponentielle de Carlitz
Soit $[i] = t^{q^i} - t$ et posons $D_n = [n]D_{n-1}^q$ avec $D_0 = 1$. On définit l'exponentielle de Carlitz comme étant l'élément de $\mathbb{F}_q((1/t))\{\{\sigma\}\}$ tel que

$$e = \sum_{i=0}^{+\infty} \frac{\sigma^i}{D_i}.$$

Définition 3.2.2 Le logarithme de Carlitz
Soit $L_n = L_{n-1}[n]$ avec $L_0 = 1$. On définit le logarithme de Carlitz λ comme étant l'élément de $\mathbb{F}_q((1/t))\{\{\sigma\}\}$ tel que

$$\lambda = \sum_{i=0}^{+\infty} \frac{(-1)^i \sigma^i}{L_i}.$$

Avec ces notations, l'élément λ est l'inverse de e : on a $e \circ \lambda = \lambda \circ e = \sigma^0$.

Proposition 3.2.1 [16]
Soit $P(t) \in \mathbb{F}_q[t]$. Alors $\gamma_P = e \circ P\sigma^0 \circ \lambda$.

Définition 3.2.3 *Supposons que $\mathcal{A}$ contient $\mathbb{F}_q[t]$. On étend la définition du module de Carlitz en posant*

$$\begin{aligned} \gamma \quad : \quad & \mathcal{A} \to K\{\{\sigma\}\} \\ & R \mapsto \gamma_R = e \circ R\sigma^0 \circ \lambda \end{aligned}$$

Cette extension s'appelle le module de Carlitz formel sur K.

Le module ainsi étendu vérifie le résultat suivant :

Théorème 3.2.1 (Hellegouarch [22])
On suppose toujours que $\mathbb{F}_q[t] \subset \mathcal{A}$. Soit $R(t) \in \mathcal{A}$. Si l'on note γ le module de Carlitz formel sur K, on a :

$$\gamma_R(T) = \sum_{i=0}^{+\infty} D^{(i)}(R)\sigma^i(T) = \sum_{i=0}^{+\infty} D^{(i)}(R)T^{q^i}.$$

Soit maintenant un module de Drinfeld Φ sur un $\mathcal{A}$-corps K et soit M le complété de K pour la topologie définie par $-\deg$. Il est montré dans [16] qu'il existe une unique série $\lambda_\Phi \in M\{\{\sigma\}\}$ telle que pour tout $P \in \mathcal{A}$ on ait :

(i) $D(\lambda) = 1$;

(ii) $\Phi_P = \lambda_\Phi^{-1} \circ P\sigma^0 \circ \lambda_\Phi$.

On note son inverse $e_\Phi = \lambda_\Phi^{-1}$. Il vérifie également $D(e) = 1$.
Ces deux séries formelles sont respectivement le logarithme et l'exponentielle du module de Drinfeld Φ. Elles permettent, de la même manière que pour le module de Carlitz, d'étendre la définition des modules de Drinfeld.

Définition 3.2.4 *Soit K un $\mathcal{A}$-corps avec $\mathbb{F}_q[t] \subset \mathcal{A}$. On appelle module de Drinfeld formel Φ sur K tout morphisme de $\mathbb{F}_q$-algèbres $\mathcal{A} \to K\{\{\sigma\}\}$ vérifiant les conditions (i) et (ii) de la définition 3.1.3. On a*

$$\begin{aligned} \Phi \quad : \quad & \mathcal{A} \to K\{\{\sigma\}\} \\ & R \mapsto \Phi_R = e_\Phi \circ R\sigma^0 \circ \lambda_\Phi \end{aligned}$$

Remarque 1 : Pour les éléments $a \in \mathcal{A}$ tels que $\Phi_a \in K\{\sigma\}$, la valeur de Φ_a donnée par la définition précédente coïncide bien avec celle que l'on obtient par le calcul $\mathbb{F}_q$-linéaire issu de Φ_t.
Remarque 2 : Soient μ et $\nu \in \mathcal{A}$. Nous avons toujours :

$$\Phi_{\mu+\nu}(T) = \Phi_\mu(T) + \Phi_\nu(T) \text{ et } \Phi_{\mu\nu}(T) = \Phi_\mu \circ \Phi_\nu(T).$$

Localisation : Soit $P(t) \in \mathbb{F}_q[t]$ irréductible et unitaire. On note $\mathbb{F}_q(t)_P$ le complété de $\mathbb{F}_q(t)$ pour la valeur absolue $P(t)$-adique. De la même manière que $\mathbb{F}_q(t)$ est l'analogue de $\mathbb{Q}$ dans les corps de séries formelles à coefficients dans $\mathbb{F}_q$, le corps $\mathbb{F}_q(t)_P$ est l'analogue du corps $\mathbb{Q}_p$ des nombres p-adiques.
Si l'on désigne par R_i les représentants de $\mathbb{F}_q[t]/(P)$ constitués par les polynômes de $\mathbb{F}_q[t]$ de degré strictement inférieur au degré de P, tout élément R de $\mathbb{F}_q(t)_P$ s'écrit :

$$R(t) = \sum_{i=n}^{+\infty} R_i(t)P(t)^i$$

avec $n \in \mathbb{Z}$. L'anneau de valuation de v_P dans $\mathbb{F}_q(t)_P$ est noté $\mathbb{F}_q[t]_P$. Tout élément R de cet anneau s'écrit :

$$R(t) = \sum_{i=0}^{+\infty} R_i(t)P(t)^i.$$

En vertu de la définition précédente, nous posons :

Définition 3.2.5 *Un module de Drinfeld formel sur $\mathbb{F}_q(t)_P$ est un homomorphisme de $\mathbb{F}_q$-algèbres*

$$\begin{array}{rccc} \Phi & : & \mathbb{F}_q[t]_P & \to & \mathbb{F}_q(t)_P\{\{\sigma\}\} \\ & & R & \mapsto & \Phi_R \end{array}$$

dont la restriction à $\mathbb{F}_q[t]$ est un module de Drinfeld sur $\mathbb{F}_q(t)$.
Le "rang de Φ" est le rang de sa restriction à $\mathbb{F}_q[t]$.

Nous avons la proposition suivante :

Proposition 3.2.2 ([27]) *Soit $R = \sum_{k=0}^{+\infty} R_k P^k \in \mathbb{F}_q[t]_P$.*

(i) *Pour tout $i \in \mathbb{N}$, la série $\sum_{k=0}^{+\infty} D^{(i)}(R_k P^k)$ est convergente dans $\mathbb{F}_q(t)_P$ et sa somme est égale à $D^{(i)}(R)$.*

(ii) *L'application $D^{(i)}$ applique $\mathbb{F}_q[t]_P$ dans lui-même.*

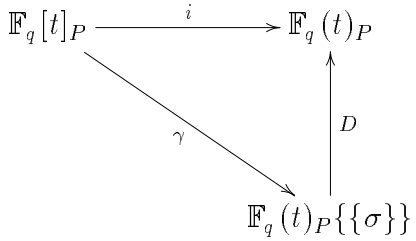
Preuve : voir [27].

Proposition 3.2.3 ([22], [27])
Soit $x \in \mathbb{F}_q[t]_P$. Les assertions suivantes sont équivalentes :

(i) $D^{(n)}(x) = 0$,

(ii) *L'élément x est un polynôme en t de degré $< n$.*

On prend maintenant $\mathcal{A} = \mathbb{F}_q[t]_P$, avec $P(t) \in \mathbb{F}_q[t]$ irréductible et unitaire, $K = \mathbb{F}_q(t)_P$ vu en tant que $\mathbb{F}_q[t]_P$-corps (le morphisme structural est l'inclusion). On peut représenter le module de Carlitz formel par le diagramme suivant :



Remarque : Le morphisme structural i étant l'inclusion, pour tout module de Drinfeld Φ défini par $\Phi_t = a_0\sigma^0 + a_1\sigma + ... + a_n\sigma^n$, la propriété $i(t) = D \circ \Phi_t = a_0$ implique $a_0 = t$.

Définition 3.2.6 *Soit γ le module de Carlitz formel sur $\mathbb{F}_q(t)_P$. On définit alors la réduction $\overline{\gamma}$ modulo P de γ par :*

$$\overline{\gamma}_R(T) = \sum_{i=0}^{+\infty} \overline{D^{(i)}}(R)T^{q^i}$$

où les $\overline{D^{(i)}}(R)$ sont les réductions modulo P des $D^{(i)}(R)$.

Remarque : Cette réduction est bien définie puisque les $D^{(i)}$ sont à valeur dans $\mathbb{F}_q[t]_P$ lorsque $R(t) \in \mathbb{F}_q[t]_P$.

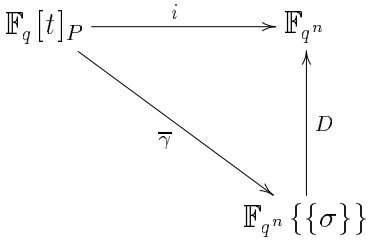
Proposition 3.2.4 *La série $\overline{\gamma}_R(T)$ est en fait une série à coefficients dans le corps $\mathbb{F}_{q^n}$ où $n = \deg(P)$.*

Preuve : De manière évidente, $\mathbb{F}_q[t]_P/(P)$ est isomorphe en tant que corps à $\mathbb{F}_q[t]/(P)$ donc à $\mathbb{F}_{q^{\deg(P)}}$.

Théorème 3.2.2 (Hayes [18])
Soit $P(t) \in \mathbb{F}_q[t]$ un polynôme irréductible, unitaire et de degré $n > 0$. Alors :

$$\gamma_P(T) \equiv T^{q^n} \pmod{P}.$$

Le diagramme ci-dessous représente la réduction modulo $P(t)$ du module de Carlitz formel sur $\mathbb{F}_q(t)_P$ où $n = \deg(P)$:



Nous pouvons faire les analogies suivantes :

$$\begin{array}{ccc}
\mathbb{Z} & \longleftrightarrow & \mathbb{F}_q[t] \\
p \text{ premier } \in \mathbb{Z} & \longleftrightarrow & P(t) \in \mathbb{F}_q[t] \text{ irréductible et unitaire} \\
\mathbb{Z}_p & \longleftrightarrow & \mathbb{F}_q[t]_P \\
\mathbb{Q}_p & \longleftrightarrow & \mathbb{F}_q(t)_P \\
r \in \mathbb{Z}_p & \longleftrightarrow & R(t) \in \mathbb{F}_q[t]_P \\
r = \sum_{i=0}^{+\infty} r_i p^i & \longleftrightarrow & R(t) = \sum_{i=0}^{+\infty} R_i(t) P(t)^i \\
0 \leq r_i \leq p-1 & \longleftrightarrow & R_i(t) \in \mathbb{F}_q[t], \deg R_i < \deg P \\
\Lambda = \{\lambda | (1+\lambda)^p - 1 = 0\} & \longleftrightarrow & \Lambda = \{\lambda | \gamma_P(\lambda) = 0\} \\
(1+T)^r - 1 & \longleftrightarrow & \gamma_R(T) \\
\sum_{i=0}^{+\infty} \left(\begin{array}{c} r \\ i \end{array} \right) T^i & \longleftrightarrow & \sum_{i=0}^{+\infty} D^{(i)}(R) T^{q^i} \\
\mathbb{F}_p = \mathbb{Z}_p / p\mathbb{Z}_p & \longleftrightarrow & \mathbb{F}_{q^{\deg P}} = \mathbb{F}_q[t]_P / P\mathbb{F}_q[t]_P
\end{array}$$

3.3 Module de Carlitz : endomorphismes algébriques

Nous avons vu au chapitre 2 que la série $(1+T)^r - 1$ réduite modulo p est algébrique sur $\mathbb{F}_p(T)$ si et seulement si r est une unité p-adique rationnelle. Nous établissons dans cette partie un analogue dans le cas où $(1+T)^r - 1$ est remplacé par $\gamma_R(T)$ avec $R(t) \in \mathbb{F}_q[t]_P$.

Proposition 3.3.1 (Allouche [2], conjecturée par Laubie)
Soit $(a_i)_{i \geq 0}$ une suite d'éléments de $\mathbb{F}_q$. Les assertions suivantes sont équivalentes :

(i) *La suite $(a_i)_{i \geq 0}$ est ultimement périodique,*

(ii) *La série $\sum_{i=0}^{+\infty} a_i T^{q^i}$ est algébrique sur $\mathbb{F}_q(T)$.*

Preuve : Posons

$$\left\{ \begin{array}{lcl} b_n & = & a_i \text{ si } n = q^i \\ b_n & = & 0 \text{ si } n \text{ n'est pas une puissance de } q \end{array} \right.$$

Alors

$$\sum_{n=0}^{+\infty} b_n T^n = \sum_{i=0}^{+\infty} a_i T^{q^i}.$$

Supposons que la série $\sum_{i=0}^{+\infty} a_i T^{q^i}$ soit algébrique sur $\mathbb{F}_q(T)$. Alors, on montre comme conséquence du théorème de [9] (voir aussi [10]) que la suite $(b_{q^n})_{n \geq 0}$ (c'est-à-dire $(a_n)_{n \geq 0}$) est ultimement périodique.

Réciproquement, si $(a_n)_n$ est ultimement périodique, montrons que $N_q(b)$ (voir définition 1.3.10) est fini. Pour tout $r \leq q^k - 1$ non nul et tout $n > 0$, $q^k n + r$ ne peut pas être une puissance de q. Donc les suites $(b_{q^k n+r})_{n\geq 0}$ avec $k \geq 0$ et $1 \leq r \leq q^k - 1$ sont nulles pour $n \geq 1$ et leur nombre est majoré par q.
Regardons maintenant les suites $(b_{q^k n})_{n\geq 0}$. Soient $C \geq 1$ et n_0 tels que pour tout $n \geq n_0$, $a_{n+C} = a_n$. La suite $(v_k(n))_n = (b_{q^k n})_n$ vérifie :

$$\begin{cases} v_k(n) &= a_{k+i} \text{ si } n = q^i, \\ v_k(n) &= 0 \text{ si } n \text{ n'est pas une puissance de } q. \end{cases}$$

Donc, pour $n \geq q^{n_0}$, on a $v_k(n) = v_{k+C}(n)$. En d'autres termes, les suites $(b_{q^k n})_n$ coïncident nécessairement pour $n \geq q^{n_0}$ avec l'une des suites v_0, v_1,...,v_{C-1}. Elles sont donc en nombre fini, majoré par Cq^{n_0+1}.
Ainsi, $N_q(b)$ est fini, et de cardinal majoré par $q + Cq^{n_0+1}$.

Lemme 3.3.1 (Cobham [11]) *Soit $(x_n)_{n\geq 0}$ une suite et soient γ et e deux entiers ≥ 1. Si l'on note*

$$N_\gamma(x) = \left\{(x_{\gamma^k n+r})_{n\geq 0}, k \geq 0, 0 \leq r \leq \gamma^k - 1\right\}$$

le γ-noyau de x, alors les assertions suivantes sont équivalentes :

(i) *Le cardinal de $N_\gamma(x)$ est fini;*

(ii) *Le cardinal de $N_{\gamma^e}(x)$ est fini.*

Preuve : Nous avons

$$N_{\gamma^e}(x) = \left\{(x_{\gamma^{ke} n+r})_{n\geq 0}, k \geq 0, 0 \leq r \leq \gamma^{ke} - 1\right\}.$$

De manière évidente, $N_{\gamma^e}(x) \subset N_\gamma(x)$ et la finitude de $N_\gamma(x)$ implique celle de $N_{\gamma^e}(x)$.
Supposons que le cardinal de $N_{\gamma^e}(x)$ est fini.
Définissons l'ensemble

$$\overline{N}_{\gamma^e}(x) = \left\{(u_{\gamma^\tau n+\alpha})_{n\geq 0}, 0 \leq \alpha \leq \gamma^e - 1, 0 \leq \tau \leq e-1, (u_n)_n \in N_{\gamma^e}(x)\right\}.$$

On a $\mathrm{Card}(\overline{N}_{\gamma^e}(x)) \leq e\gamma^e \mathrm{Card}(N_{\gamma^e}(x))$ et ainsi $\overline{N}_{\gamma^e}(x)$ est fini.
Soit $y \in N_\gamma(x)$: $(y_n)_{n\geq 0} = (x_{\gamma^a n+r})_{n\geq 0} \in N_\gamma(x)$ avec $a \geq 0$ et $0 \leq r \leq \gamma^a - 1$ et écrivons $a = \beta e + \tau$ avec $0 \leq \tau \leq e-1$ et $\beta \in \mathbb{N}$. Alors $(y_n)_n = (x_{\gamma^{\beta e}\gamma^\tau n+r})_n$ avec $r < \gamma^\tau \gamma^{\beta e}$.
Comme $\tau < e$, on peut écrire que $r < \gamma^e \gamma^{\beta e}$. Donc $r = \alpha\gamma^{\beta e} + r'$ avec $\alpha < \gamma^e$ et $0 \leq r' \leq \gamma^{\beta e} - 1$.
D'où :

$$\begin{aligned} (y_n)_n &= (x_{\gamma^{\beta e}\gamma^\tau n+\alpha\gamma^{\beta e}+r'})_n \\ &= (x_{\gamma^{\beta e}(\gamma^\tau n+\alpha)+r'})_n \\ &= (z_{\gamma^\tau n+\alpha})_n \text{ avec } (z_n)_n \in N_{\gamma^e}(x), \alpha < \gamma^e \text{ et } \tau < e. \end{aligned}$$

On en déduit que $(y_n)_n \in \overline{N}_{\gamma^e}(x)$. Ainsi $N_\gamma(x) \subset \overline{N}_{\gamma^e}(x)$ qui est fini. D'où la conclusion.

Proposition 3.3.2 *Soient q une puissance d'un nombre premier p, $r = q^\alpha$ avec $\alpha \in \mathbb{N}^*$ et $(a_n)_{n\geq 0} \in \mathbb{F}_r^{\mathbb{N}}$. Les assertions suivantes sont équivalentes :*

(i) *La suite $(a_n)_{n\geq 0}$ est ultimement périodique,*

(ii) *La série $\sum_{n\geq 0} a_n T^{q^n}$ est algébrique sur $\mathbb{F}_r(T)$.*

Preuve : Par la proposition précédente, l'ultime périodicité de la suite $(a_n)_{n\geq 0}$ est équivalente à l'algébricité sur $\mathbb{F}_r(T)$ de la série $\sum_{i=0}^{+\infty} a_i T^{r^i}$.

Nous allons montrer que la série $\sum_{i=0}^{+\infty} a_i T^{q^i} \in \mathbb{F}_r[[T]]$ est algébrique sur $\mathbb{F}_r(T)$ si et seulement si la série $\sum_{i=0}^{+\infty} a_i T^{r^i}$ est algébrique sur $\mathbb{F}_r(T)$.

Nous nous proposons de montrer cette équivalence de deux manières différentes, l'une utilisant les q-noyaux, l'autre proposée par Y. Hellegouarch et utilisant le fait que les séries $\sum a_i T^{r^i}$ et $\sum a_i T^{q^i}$ sont images l'une de l'autre par un endomorphisme continu de $\mathbb{F}_r[[T]]$.

Méthode 1 :

Définissons les suites $(b_n)_{n\geq 0}$ et $(b'_n)_{n\geq 0}$ à valeurs dans $\mathbb{F}_r$ par :

$$\begin{cases} b_n &= a_i \text{ si } n = q^i, \\ b_n &= 0 \text{ si } n \text{ n'est pas une puissance de } q, \end{cases}$$

$$\begin{cases} b'_n &= a_i \text{ si } n = r^i, \\ b'_n &= 0 \text{ si } n \text{ n'est pas une puissance de } r. \end{cases}$$

On a alors

$$\sum_{i=0}^{+\infty} a_i T^{r^i} = \sum_{n=0}^{+\infty} b'_n T^n \in \mathbb{F}_r[[T]]$$

et

$$\sum_{i=0}^{+\infty} a_i T^{q^i} = \sum_{n=0}^{+\infty} b_n T^n \in \mathbb{F}_r[[T]].$$

On est ramené à montrer que $\sum_{n=0}^{+\infty} b'_n T^n$ est algébrique sur $\mathbb{F}_r(T)$ si et seulement si $\sum_{n=0}^{+\infty} b_n T^n$ est algébrique sur $\mathbb{F}_r(T)$.

Montrons tout d'abord que le r-noyau de (b'_n) est fini si et seulement si le q-noyau de (b_n) est fini.

Soit $(x_n)_{n\geq 0} \in N_r((b'_n)_{n\geq 0})$. Alors il existe $k \geq 0$ et $\rho \in [0, ..., r^k - 1]$ tels que $x_n = b'_{r^k n+\rho}$ pour $n \geq 0$. Si $\rho > 0$, pour tout $n > 0$, $r^k n + \rho$ ne peut pas être une puissance de r.

D'où, pour $\rho > 0$, les suites $n \mapsto b'_{r^k n+\rho}$ sont nulles pour $n \geq 1$. Le nombre de ces suites est majoré par r.
On en déduit que la finitude du cardinal de $N_r((b'_n)_{n\geq 0})$ est équivalente à la finitude du cardinal de l'ensemble

$$N'_r((b'_n)) = \left\{(b'_{r^k n})_{n\geq 0}, k \geq 0\right\}.$$

De même, le q-noyau $N_q((b_n)_{n\geq 0})$ est fini si et seulement si le cardinal de l'ensemble

$$N'_q((b_n)) = \left\{(b_{q^k n})_{n\geq 0}, k \geq 0\right\}$$

est fini.
Soient k_1 et k_2 deux entiers vérifiant $((b'_{r^{k_1} n})_{n\geq 0}) = ((b'_{r^{k_2} n})_{n\geq 0})$.
Nous avons la succession d'équivalences :

$$\begin{aligned}
((b'_{r^{k_1} n})_{n\geq 0}) = ((b'_{r^{k_2} n})_{n\geq 0}) &\Leftrightarrow \forall n = r^u, b'_{r^{k_1+u}} = b'_{r^{k_2+u}} \\
&\Leftrightarrow \forall n = r^u, a_{k_1+u} = a_{k_2+u} \\
&\Leftrightarrow \forall u \in \mathbb{N}, a_{k_1+u} = a_{k_2+u} \\
&\Leftrightarrow \forall n = q^u, b_{q^{k_1+u}} = b_{q^{k_2+u}} \\
&\Leftrightarrow ((b_{q^{k_1} n})_{n\geq 0}) = ((b_{q^{k_2} n})_{n\geq 0})
\end{aligned}$$

On en déduit que $N'_r((b'_n)_{n\geq 0})$ et $N'_q((b_n)_{n\geq 0})$ ont même cardinal et donc que le r-noyau de $(b'_n)_{n\geq 0}$ est fini si et seulement si le q-noyau de $(b_n)_{n\geq 0}$ est fini. D'après le lemme 3.3.1, la dernière assertion est équivalente à dire que le r-noyau de $(b_n)_{n\geq 0}$ est fini, d'où la conclusion.
Méthode 2 :
Posons $\sigma : x \mapsto x^q$. Il est clair, avec les notations de l'énoncé, que $x^r = \sigma^\alpha(x)$. De plus, σ est un endomorphisme continu de $\mathbb{F}_r[[T]]$. Par ailleurs, σ est un automorphisme de $\mathbb{F}_r$ (d'ordre α). Il s'agit de montrer que $\theta = \sum_{n=0}^{\infty} a_n T^{q^n}$ est algébrique sur $\mathbb{F}_r(T)$ si et seulement si $\omega = \sum_{n=0}^{\infty} a_n T^{r^n}$ est algébrique sur $\mathbb{F}_r(T)$.
Si θ est algébrique sur $\mathbb{F}_r(T)$, on a :

$$\theta^d + b_1(T)\theta^{d-1} + ... + b_d(T) = 0,\ d > 0, \text{ avec } b_i(T) \in \mathbb{F}_r(T).$$

On en déduit que $\omega = \sigma^\alpha(\theta)$ est algébrique sur $\mathbb{F}_r(T)$, car $\sigma^\alpha(b_i(T)) = b_i(T^r) \in \mathbb{F}_r(T)$.
Inversement, si ω est algébrique sur $\mathbb{F}_r(T)$, on a :

$$\omega^e + c_1(T)\omega^{e-1} + ... + c_e(T) = 0,\ e > 0, \text{ avec } c_j(T) \in \mathbb{F}_r(T)$$

et cela s'écrit :

$$\theta^{re} + c_1(T)\theta^{re-r} + ... + c_e(T) = 0.$$

Proposition 3.3.3 *Soit $P(t) \in \mathbb{F}_q[t]$ irréductible, unitaire, de degré n et soit $R(t) \in \mathbb{F}_q[t]$ tel que $\deg(R) < n$. Pour $k \in \mathbb{N}^*$, on a :*

$$\begin{aligned} D^{(i)}(RP^k) &\equiv 0 \pmod{P} \text{ si } i < kn \\ &\equiv D^{(i-kn)}(R) \pmod{P} \text{ si } kn \leq i < (k+1)n \\ &\equiv 0 \pmod{P} \text{ si } (k+1)n \leq i. \end{aligned}$$

Preuve : On sait, d'après le théorème 3.2.2, que

$$\gamma_P(T) \equiv T^{q^n} \pmod{P}.$$

Donc

$$\gamma_{P^k}(T) = \underbrace{\gamma_P \circ \gamma_P \circ ... \circ \gamma_P(T)}_{k \text{ fois}} \equiv T^{q^{kn}} \pmod{P}.$$

Or $\gamma_{P^k}(T) = \sum_{i=0}^{kn} D^{(i)}(P^k) T^{q^i} \equiv T^{q^{kn}} \pmod{P}$. D'où pour $i < kn$, on a par identification $D^{(i)}(P^k) \equiv 0 \pmod{P}$.
Toujours pour $i < kn$ et en utilisant la formule de Leibniz, il vient :

$$D^{(i)}(RP^k) = D^{(i)}(P^k R) = \sum_{j=0}^{i} D^{(j)}(P^k) \left(D^{(i-j)}(R)\right)^{q^j}.$$

Or pour $j = 0, ..., i$, on a $D^{(j)}(P^k) \equiv 0 \pmod{P}$, d'où

$$D^{(i)}(RP^k) \equiv 0 \pmod{P}.$$

Supposons maintenant que $i \geq kn$. On a

$$D^{(i)}(RP^k) = \sum_{j=0}^{i} D^{(j)}(R) \left(D^{(i-j)}(P^k)\right)^{q^j}.$$

Si $i - j < kn$, on a vu que $D^{(i-j)}(P^k) \equiv 0 \pmod{P}$.
Si $i - j > kn$, alors $D^{(i-j)}(P^k) = 0$ car $i - j > \deg(P^k)$. D'où :

$$D^{(i)}(RP^k) \equiv D^{(i-kn)}(R) \pmod{P}.$$

Enfin si $i \geq (k+1)n$ alors $i > \deg(RP^k)$ et

$$D^{(i)}(RP^k) = 0.$$

D'où les trois congruences de la proposition.
Remarque : On peut également obtenir ces congruences en tant que corollaire de la proposition de [23].

Théorème 3.3.1 *Soit un polynôme $P(t) \in \mathbb{F}_q[t]$ irréductible, unitaire, de degré n et soit*

$$R(t) = \sum_{k=0}^{+\infty} R_k(t)P(t)^k \in \mathbb{F}_q[t]_P$$

(avec $\deg(R_k) < n$). Les assertions suivantes sont équivalentes :

(i) *La série $R(t)$ est dans $\mathbb{F}_q(t)$,*

(ii) *La série $\overline{\gamma_R}(T) \in \mathbb{F}_{q^n}[[T]]$ est algébrique sur $\mathbb{F}_{q^n}(T)$.*

Preuve : Nous avons

$$\gamma_R(T) = \sum_{i=0}^{+\infty} D^{(i)}(R)T^{q^i}$$

avec

$$R(t) = \sum_{k=0}^{+\infty} R_k(t)P(t)^k$$

et

$$D^{(i)}(R) = \sum_{k=0}^{+\infty} D^{(i)}(R_kP^k) \text{ pour } i \in \mathbb{N}.$$

Par la suite, on note $E(x)$ le plus petit entier inférieur ou égal à x. Soit $i \in \mathbb{N}$ et soit $k_0 = E(i/n)$. Alors $k_0 n \leq i < (k_0+1)n$.
Soit $k \neq k_0$, alors $i \notin [kn, (k+1)n[$ et dans ce cas, d'après la proposition 3.3.3, on a :

$$D^{(i)}(R_kP^k) \equiv 0 \pmod{P}.$$

De plus, d'après le même lemme $D^{(i)}(R_{k_0}P^{k_0}) \equiv D^{(i-k_0n)}(R_{k_0}) \pmod{P}$. D'où :

Lemme 3.3.2

$$D^{(i)}(R) \equiv D^{(i-k_0n)}(R_{k_0}) \pmod{P}. \tag{3.1}$$

Par la proposition 3.3.2, il nous suffit d'établir que la suite $(R_k)_{\geq 0}$ est ultimement périodique de période $h \geq 1$ si et seulement si la suite

$$\left(\overline{D^{(i)}}(R)\right)_{i\geq 0} = \left(D^{(i)}(R) \bmod P\right)_{i\geq 0}$$

est ultimement périodique de période hn.
Soit h une période de la suite $(R_k)_{k\geq 0}$. Pour $i \in \mathbb{N}$, évaluons la quantité $D^{(i+hn)}(R)$.
Soit $k_0' = E\left(\dfrac{i+hn}{n}\right)$: $k_0'n \leq i + hn < (k_0'+1)n$. Il vient, en posant $j = i + hn$,

$$D^{(j)}(R) \equiv D^{(j-k_0'n)}\left(R_{E(j/n)}\right) \pmod{P}.$$

Clairement, $k_0' = k_0 + h$ et $j - k_0'n = i - k_0 n$. Nous obtenons à partir d'un certain rang :

$$\begin{aligned} D^{(j)}(R) &\equiv D^{(j-k_0'n)}(R_{E(i/n)+h}) \pmod P \text{ (car } k_0' = k_0 + h) \\ &\equiv D^{(j-k_0'n)}(R_{E(i/n)}) \pmod P \text{ (car } (R_k)_k \text{ est de période } h) \\ &\equiv D^{(i-k_0 n)}(R_{E(i/n)}) \pmod P \text{ (car } j - k_0'n = i - k_0 n) \\ &\equiv D^{(i)}(R) \pmod P \text{ (d'après le lemme 3.3.2).} \end{aligned}$$

D'où $D^{(j)}(R) = D^{(i+hn)}(R) \equiv D^{(i)}(R) \pmod P$ et hn est une période de la suite $\left(\overline{D^{(i)}}(R)\right)_{i\geq 0}$.
Réciproquement, supposons que $D^{(i+hn)}(R) \equiv D^{(i)}(R) \pmod P$ pour tout i supérieur ou égal à un certain i_0. On pose $j = i + hn$ puis $k_0 = E(i/n)$ et $k_0' = E(j/n)$.
Pour $i \geq i_0$, d'après le lemme 3.3.2,

$$D^{(i)}(R) \equiv D^{(i-k_0 n)}(R_{k_0}) \pmod P$$

et

$$D^{(i+hn)}(R) \equiv D^{(j-k_0'n)}(R_{k_0'}) \pmod P.$$

Nous avons $j - k_0'n = i - k_0 n$. D'où

$$D^{(i-k_0 n)}(R_{k_0}) \equiv D^{(i-k_0 n)}(R_{k_0+h}) \text{ (car } k_0' = k_0 + h).$$

Cette congruence est vraie en particulier si $i = k_0 n$ car pour cette valeur, on a encore $E(i/n) = k_0$ et $E((i + hn)/n) = k_0'$. On obtient par $\mathbb{F}_q$-linéarité :

$$D^{(0)}(R_{k_0} - R_{k_0+h}) \equiv 0 \pmod P.$$

Comme $D^{(0)}(R_{k_0} - R_{k_0+h}) = R_{k_0} - R_{k_0+h}$, il vient

$$R_{k_0} - R_{k_0+h} \equiv 0 \pmod P.$$

De plus, comme $\deg(R_k) < n$ pour tout k, $\deg(R_{k_0} - R_{k_0+h}) < n = \deg(P)$. On en déduit bien que $R_{k_0} = R_{k_0+h}$.

3.4 Cas des modules de Drinfeld de rang 1

Nous allons étendre les conclusions du théorème 3.3.1 aux modules de Drinfeld de rang 1.
Soit Φ un module de Drinfeld formel de rang 1 défini sur $\mathbb{F}_q[t]_P$ et soit γ le module de Carlitz formel.
Cherchons un isomorphisme entre Φ et γ. Il sera de la forme $\mu = \alpha\sigma^0$ avec α appartenant à une clôture algébrique de $\mathbb{F}_q(t)_P$.
Si l'on écrit $\gamma_t = t\sigma^0 + \sigma$ et $\Phi_t = t\sigma^0 + a\sigma$ avec $a \in \mathbb{F}_q[t]_P$, il vient :

$$\mu\Phi_t = \gamma_t\mu$$

puis

$$\begin{aligned}\Phi_t &= \mu^{-1}\gamma_t\mu \\ &= \alpha^{-1}(t\alpha\sigma^0 + \alpha^q\sigma) \\ &= t\sigma^0 + \alpha^{q-1}\sigma.\end{aligned}$$

On en déduit que $\alpha = a^{1/(q-1)}$ et que son polynôme minimal $F(X)$ sur $\mathbb{F}_q(t)_P$ divise $X^{q-1} - a$.
Posons $K = \mathbb{F}_q(t)_P$, $A = \mathbb{F}_q[t]_P$ et $\overline{K} = A/(P) \simeq \mathbb{F}_{q^n}$ où n est le degré de P.
Remarquons que si $a \equiv 0 \pmod P$ alors $\overline{\Phi}_R(T) = uT$ avec $u \in \overline{K}$ pour tout $R(t) \in A$ et que dans ce cas le problème de l'algébricité ne se pose pas. Nous nous intéressons dorénavant aux modules de Drinfeld de rang 1 de réduction non triviale, c'est-à-dire tels que $a \not\equiv 0 \pmod P$.

Lemme 3.4.1 *Soit $F(X) \in A[X]$ le polynôme minimal de α sur K. Si $\overline{F}(X)$ représente le polynôme $F(X)$ dont les coefficients ont été projetés dans le corps résiduel $\overline{K}$, alors $\overline{F}(X)$ est irréductible sur $\overline{K}[X]$.*

Preuve : On écrit $G(X) = X^{q-1} - a = F(X)Q(X)$ avec $Q(X) \in A[X]$.
Si l'on pose $a = a_0(t) + a_1(t)P(t) + a_2(t)P(t)^2 + ...$ avec les $a_i(t)$ de degré inférieur strictement au degré de $P(t)$, il vient $\overline{G}(X) = X^{q-1} - a_0 \in \overline{K}[X]$.
Comme $\overline{G}'(X) = (q-1)X^{q-2}$, on voit que $\overline{G}(X)$ n'a que des racines simples. Ceci implique que $\overline{F}(X)$ n'a également que des racines simples et que s'il existe $e(X)$ et $f(X) \in \overline{K}[X]$ tels que $\overline{F}(X) = e(X)f(X)$ alors e et f sont premiers entre eux.
Par le lemme de Hensel [6], on en déduit que $F(X)$ se factorise dans $A[X]$, ce qui est contraire aux hypothèses.

Théorème 3.4.1 *Soit Φ un module de Drinfeld de rang 1 défini sur $\mathbb{F}_q[t]_P$ et soit $R(t) \in \mathbb{F}_q[t]_P$. On suppose que Φ est de réduction modulo P non triviale. Si l'on pose $n = \deg(P)$, les assertions suivantes sont équivalentes :*

(i) *La série $R(t)$ est dans $\mathbb{F}_q(t)$;*

(ii) *La série $\overline{\Phi}_R(T)$ est algébrique sur $\mathbb{F}_{q^n}(T)$.*

Preuve : D'après le lemme précédent, on sait que l'image $\overline{F}(X)$ de $F(X)$ dans $\overline{K}[X]$ est un polynôme irréductible. On en déduit que l'idéal (P) reste maximal dans l'anneau de valuation de $K' = K(\alpha)$ et que $\overline{\alpha} = \alpha \bmod P \in \overline{K'}$ où $\overline{K'}$ est le corps résiduel de K'. Ainsi $\overline{\alpha} \in \mathbb{F}_r$ où r est une puissance de q^n.
Les séries $\overline{\Phi}_R(T)$ et $\overline{\gamma}_R(T)$ qui sont à coefficients dans $\mathbb{F}_{q^n}$ peuvent être vues comme étant des séries à coefficients dans $\mathbb{F}_r$. L'algébricité de $\overline{\Phi}_R(T) = \overline{\mu}^{-1}\overline{\gamma}_R\overline{\mu}(T)$ sur $\mathbb{F}_r(T)$ (donc sur $\mathbb{F}_{q^n}(T)$) est alors équivalente à celle de $\overline{\gamma}_R(T)$.

3.5 Construction explicite des endomorphismes

Nous allons voir dans cette partie une construction récurrente d'endomorphismes de modules de Drinfeld formels sur $\mathbb{F}_q(t)_p$. Nous donnons ensuite, dans le cas des modules

réduits de rang 1, une condition nécessaire et suffisante pour que la suite des coefficients soit p-automatique.

Soit $P(t) \in \mathbb{F}_q[t]$ irréductible et unitaire.

Proposition 3.5.1 *Soit Φ un module de Drinfeld formel sur $\mathbb{F}_q(t)_P$ et soit $R(t) \in \mathbb{F}_q[t]_P$. On suppose que $\Phi_t = t\sigma^0 + d_1\sigma + ... + d_\delta\sigma^\delta \in \mathbb{F}_q[t]_P\{\sigma\}$. Alors il existe un unique élément $\Phi_R = \sum_{i=0}^{+\infty} \Delta^{(i)}(R)\sigma^i \in \mathbb{F}_q(t)_P\{\{\sigma\}\}$ tel que :*

$$\begin{array}{rcl} \Phi_R & \equiv & R\sigma^0 \pmod{\sigma}, \\ \Phi_t\Phi_R & = & \Phi_R\Phi_t. \end{array}$$

Si l'on pose $\Phi_R^j = \sum_{i=0}^{j-1} \Delta^{(i)}(R)\sigma^i$, alors :

$$\Delta^{(i)}(R)\sigma^i = \frac{\Phi_t\Phi_R^i - \Phi_R^i\Phi_t}{t^{q^i} - t} \bmod \sigma^{i+1} \in \mathbb{F}_q(t)_P\sigma^i.$$

Preuve : On va montrer par récurrence sur i que le système

$$\left\{ \begin{array}{rcl} \Phi_R^i & \equiv & R\sigma^0 \pmod{\sigma}, \\ \Phi_t\Phi_R^i & \equiv & \Phi_R^i\Phi_t \pmod{\sigma^i} \end{array} \right.$$

admet une unique solution Φ_R^i, polynôme en σ de degré $i-1$. Pour $i = 1$, posons $\Phi_R^1 = R\sigma^0 = \Delta^{(0)}(R)\sigma^0$. Il vient alors immédiatement :

$$\left\{ \begin{array}{rcl} \Phi_R^1 & \equiv & R\sigma^0 \pmod{\sigma}, \\ \Phi_t\Phi_R^1 & \equiv & \Phi_R^1\Phi_t \pmod{\sigma}. \end{array} \right.$$

Soit $i \geq 2$. Cherchons Φ_R^{i+1} sous la forme $\Phi_R^{i+1} = \Phi_R^i + \Delta^{(i)}(R)\sigma^i$. On a

1) $\Phi_t\Phi_R^{i+1} = \Phi_t\Phi_R^i + \Phi_t\Delta^{(i)}(R)\sigma^i \equiv \Phi_t\Phi_R^i + t\Delta^{(i)}(R)\sigma^i \pmod{\sigma^{i+1}}$,

2) $\Phi_R^{i+1}\Phi_t = \Phi_R^i\Phi_t + \Delta^{(i)}(R)\sigma^i\Phi_t \equiv \Phi_R^i\Phi_t + \Delta^{(i)}(R)\sigma^i(t\sigma^0) \pmod{\sigma^{i+1}}$.

D'où :

$$\Phi_t\Phi_R^i - \Phi_R^i\Phi_t \equiv \Delta^{(i)}(R)t^{q^i}\sigma^i - \Delta^{(i)}(R)t\sigma^i \pmod{\sigma^{i+1}}$$

et enfin :

$$\Delta^{(i)}(R)\sigma^i \equiv \frac{\Phi_t\Phi_R^i - \Phi_R^i\Phi_t}{t^{q^i} - t} \pmod{\sigma^{i+1}}.$$

Remarque : Si $\delta = 1$, il est facile de voir que les séries $\Phi_R(T)$ sont dans $\mathbb{F}_q[t]_P[[T]]$. Il suffit pour cela de remarquer tout d'abord que si $\Phi_t = t\sigma^0 + \sigma$, le résultat est vrai car on retrouve les dérivées galoisiennes. Maintenant, si $\Phi_t = t\sigma^0 + a\sigma$ avec $a \in \mathbb{F}_q[t]_P$, on montre facilement par récurrence sur i que $\Delta^{(i)}(R) = a\sigma(a)\sigma^2(a)...\sigma^{i-1}(a)D^{(i)}(R) \in \mathbb{F}_q[t]_P$.

Corollaire 3.5.1 *Soit Φ un module de Drinfeld formel de rang 1 sur $\mathbb{F}_q(t)_p$ vérifiant les hypothèses de la proposition précédente. Si $\Phi_t = t\sigma^0 + a\sigma$, la série $\Phi_R = \sum_{i=0}^{+\infty} \Delta^{(i)}(R)\sigma^i$ peut être définie par la récurrence :*

$$\Delta^{(0)}(R) = R,$$
$$\Delta^{(i)}(R) = \frac{a\Delta^{(i-1)}(R)^q - a^{q^{i-1}}\Delta^{(i-1)}(R)}{t^{q^i} - t}.$$

Preuve : On part de l'égalité $\Delta^{(i)}(R)\sigma^i = \dfrac{\Phi_t\Phi_R^i - \Phi_R^i\Phi_t}{t^{q^i} - t} \bmod \sigma^{i+1}$.
La série $\Phi_t\Phi_R^i - \Phi_R^i\Phi_t$ étant d'ordre i en σ, il suffit, pour le calcul de $\Delta^{(i)}(R)$ de calculer le coefficient de σ^i dans la fraction ci-dessus.
En écrivant $\Phi_R^i = \Delta^{(0)}(R)\sigma^0 + \Delta^{(1)}(R)\sigma + ... + \Delta^{(i-1)}(R)\sigma^{i-1}$, on voit que le coefficient en question est :

$$\begin{aligned}\Delta^{(i)}(R) &= \frac{a\sigma(\Delta^{(i-1)}(R)\sigma^{i-1}) - \Delta^{(i-1)}(R)\sigma^{i-1}(a)}{t^{q^i} - t} \times \frac{1}{\sigma^i} \\ &= \frac{a\Delta^{(i-1)}(R)^q - a^{q^{i-1}}\Delta^{(i-1)}(R)}{t^{q^i} - t}.\end{aligned}$$

Corollaire 3.5.2 *Le module γ de Carlitz formel sur $\mathbb{F}_q(t)_P$ admet pour endomorphismes les séries $\gamma_R = \sum_{i=0}^{+\infty} \Delta^{(i)}(R)\sigma^i$ avec*

$$\Delta^{(0)}(R) = R,$$
$$\Delta^{(i)}(R) = \frac{\Delta^{(i-1)}(R)^q - \Delta^{(i-1)}(R)}{t^{q^i} - t}.$$

Preuve : Il suffit de prendre $a = 1$ dans le corollaire précédent.

Corollaire 3.5.3 *Soit Φ un module de Drinfeld formel sur $\mathbb{F}_q(t)_P$ de rang δ avec*

$$\Phi_t = \sum_{k=0}^{\delta} d_k\sigma^k \text{ (où } d_0 = t \text{ et } d_k \in \mathbb{F}_q[t]_P \text{ pour } k = 1, 2, ..., \delta).$$

Pour $R(t) \in \mathbb{F}_q[t]_P$, si l'on note $\Phi_R = \sum_{i=0}^{+\infty} \Delta^{(i)}(R)\sigma^i$, alors la suite $(\Delta^{(i)}(R))_{i\geq 1}$ peut être caractérisée par une récurrence d'ordre δ et on a :

$$\Delta^{(i)}(R) = \sum_{k=1}^{\delta} \frac{d_k\left(\Delta^{(i-k)}(R)\right)^{q^k} - d_k^{q^{i-k}}\Delta^{(i-k)}(R)}{t^{q^i} - t}.$$

Preuve : Le coefficient de σ^i dans $\dfrac{\Phi_t\Phi_R^i - \Phi_R^i\Phi_t}{t^{q^i}-t}$ est alors

$$\left(\frac{d_1\sigma(\Delta^{(i-1)}\sigma^{i-1}) + d_2\sigma^2(\Delta^{(i-2)}\sigma^{i-2}) + \ldots + d_\delta\sigma^\delta(\Delta^{(i-\delta)}\sigma^{i-\delta})}{t^{q^i}-t} - \right.$$

$$\left.\frac{\Delta^{(i-1)}\sigma^{i-1}(d_1\sigma) + \Delta^{(i-2)}\sigma^{i-2}(d_2\sigma^2) + \ldots + \Delta^{(i-\delta)}\sigma^{i-\delta}(d_\delta\sigma^\delta)}{t^{q^i}-t}\right) \times \frac{1}{\sigma^i},$$

d'où la conclusion.

Nous terminons ce chapitre en donnant, dans le cas des modules de rang 1, une condition nécessaire et suffisante pour que les suites $(\overline{\Delta}^{(i)}(R))_{i\geq 0}$ soient p-automatiques.

Théorème 3.5.1 *Soit un polynôme $P(t) \in \mathbb{F}_q[t]$ irréductible, unitaire et de degré n, soit $R(t) = \sum_{k=0}^{+\infty} R_k(t)P(t)^k \in \mathbb{F}_q[t]_P$ et soit $a \in \mathbb{F}_q[t]_P$ tel que $a \not\equiv 0 \pmod P$.*
Soit $\left(\Delta^{(i)}(R)\right)_i$ une suite vérifiant la récurrence

$$\begin{aligned}\Delta^{(0)}(R) &= R,\\ \Delta^{(i)}(R) &= \frac{a\Delta^{(i-1)}(R)^q - a^{q^{i-1}}\Delta^{(i-1)}(R)}{t^{q^i}-t},\end{aligned}$$

et soit ψ l'application $\mathbb{F}_q$-linéaire définie par

$$\begin{array}{rccl}\psi & : & \mathbb{F}_q[t]_P & \to & \mathbb{F}_{q^n}[[T]]\\ & & R(t) & \mapsto & \displaystyle\sum_{i=0}^{\infty}\overline{\Delta^{(i)}}(R)T^i.\end{array}$$

Les assertions suivantes sont équivalentes :

(i) *La suite $(R_k(t))_k$ est p-automatique;*

(ii) *La suite $(\overline{\Delta}^{(i)}(R))_i = (\Delta^{(i)}(R) \bmod P)_i$ est p-automatique;*

(iii) *La série $(\psi(R))(T)$ est algébrique sur sur $\mathbb{F}_{q^n}(T)$.*

Remarque : L'assertion (i) évoque la notion de p-noyau d'une suite de polynômes. Notons ici que cette notion a bien un sens : en effet, chaque polynôme $R_k(t)$ est à coefficients dans $\mathbb{F}_q$ et est de degré strictement inférieur à n. Ceci implique que l'on peut voir les $R_k(t)$ comme étant les éléments d'un alphabet à q^n éléments. On peut alors calculer le p-noyau de la suite $(R_k(t))_{k\geq 0}$.

Preuve du théorème :
L'équivalence entre les assertions (ii) et (iii) est évidente. Montrons que (i) est équivalente à (ii). On commence par établir le résultat dans le cas où $\Delta^{(i)}$ est la

$i^{\text{ième}}$ dérivée galoisienne $D^{(i)}$.
Soit $k \in \mathbb{N}$ tel que $k \leq n-1$. D'après la proposition 3.3.3, on a pour tout $u \in \mathbb{N}$:

$$D^{(un+k)}(R) \equiv D^{(k)}(R_u) \pmod{P}. \tag{3.2}$$

Supposons que la suite $(R_u)_{u\geq 0}$ est q^n-automatique. Alors la suite $(\overline{D}^{(k)}(R_u))_{u\geq 0}$ l'est également. Par la congruence 3.2, la suite $\left(\overline{D}^{(un+k)}(R)\right)_{u\geq 0}$ est q^n-automatique. Ceci est équivalent à affirmer que la série

$$\sum_{u=0}^{+\infty} \overline{D}^{(un+k)}(R)T^u \in \mathbb{F}_{q^n}[[T]]$$

est algébrique sur $\mathbb{F}_{q^n}(T)$.
En composant à droite par T^n, il vient :

$$\sum_{u=0}^{+\infty} \overline{D}^{(un+k)}(R)T^{un} \text{ est algébrique sur } \mathbb{F}_{q^n}(T)$$

puis en multipliant par T^k :

$$\sum_{u=0}^{+\infty} \overline{D}^{(un+k)}(R)T^{un+k} \text{ est algébrique.}$$

Ce résultat est vrai pour $k = 0, ..., n-1$.

Si l'on ajoute les n séries algébriques, on obtient l'algébricité de la série $\displaystyle\sum_{i=0}^{+\infty} \overline{D}^{(i)}(R)T^i$ sur $\mathbb{F}_{q^n}(T)$ vue en tant que somme finie de séries algébriques. Ceci signifie que la suite $\left(\overline{D}^{(i)}(R)\right)_{i\geq 0}$ est q^n-automatique.

Réciproquement, si la suite $\left(\overline{D^{(u)}}(R)\right)_{u\geq 0}$ est q^n-automatique, alors la sous-suite $\left(\overline{D^{(un)}}(R)\right)_{u\geq 0}$ l'est aussi (voir par exemple [4]).
Or, par la proposition 3.3.3, on sait que $D^{(un)}(R) \equiv D^{(0)}(R_u) \pmod{P}$. On en déduit la q^n-automaticité de la suite $\left(\overline{D^{(0)}}(R_u)\right)_{u\geq 0} = (R_u)_{u\geq 0}$.

Dans le cas général, on part d'un isomorphisme μ entre un module formel Φ de rang 1 et le module de Carlitz formel. L'égalité

$$\Phi_R = \mu^{-1}\gamma_R\mu \text{ où } \mu = \alpha\sigma^0$$

implique par $\mathbb{F}_q$-linéarité :

$$\Delta^{(i)}(R) = \alpha^{-1}D^{(i)}(R)\alpha^{q^i} = \alpha^{q^i-1}D^{(i)}(R).$$

Comme $\alpha = a^{1/(q-1)}$, il vient

$$\Delta^{(i)}(R) = a^{\frac{q^i-1}{q-1}}D^{(i)}(R) = a^{1+q+q^2+...+q^{i-1}}D^{(i)}(R) = aa^qa^{q^2}...a^{q^{i-1}}D^{(i)}(R).$$

Notons u_i la réduction modulo P de $aa^qa^{q^2}...a^{q^{i-1}}$ et établissons le lemme suivant :

Lemme 3.5.1 *La suite $(u_i)_{i\geq 0}$ est périodique de période $(q-1)n$.*

Preuve : Soit $i \in \mathbb{N}$. Si l'on note $\overline{a}$ la réduction de a modulo P, alors $\overline{a} \in \mathbb{F}_{q^n}$ et nous avons :

$$\begin{aligned} u_{i+(q-1)n} &= u_i \left(N_{\mathbb{F}_{q^{(q-1)n}}/\mathbb{F}_q}(\overline{a})\right)^{q^i} \\ &= u_i \left(N_{\mathbb{F}_{q^{(q-1)n}}/\mathbb{F}_q}(\overline{a})\right) \\ &= u_i \left(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\overline{a})\right)^{q-1} \\ &= u_i \end{aligned}$$

car $\overline{a} \neq \overline{0}$ et $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\overline{a}) \in \mathbb{F}_q^*$.

Revenons à la démonstration du théorème. Nous avons

$$\overline{\Delta^{(i)}}(R) = u_i \overline{D^{(i)}}(R).$$

Supposons que la suite $\left(\overline{D^{(i)}}(R)\right)_{i\geq 0}$ est q^n-automatique. La suite $(u_i)_{i\geq 0}$ étant périodique, la série $\sum_{i\geq 0} u_i T^i$ est rationnelle, donc algébrique, ce qui signifie que la suite $(u_i)_{i\geq 0}$ est q^n-automatique. Par le théorème 1.4.4, la suite $\left(\overline{\Delta^{(i)}}(R)\right)_{i\geq 0}$ est alors q^n-automatique en tant que produit de Hadamard de deux suites q^n-automatiques. Remarquons au passage que, le corps des coefficients étant un corps fini, on peut obtenir la q^n-automaticité du produit de Hadamard sans nécessairement utiliser le théorème 1.4.4 qui est très général, mais simplement en constatant que si v_1 et v_2 sont deux suites, alors $Card(N_{q^n}(v_1 * v_2)) \leq Card(N_{q^n}(v_1))Card(N_{q^n}(v_2))$.

Réciproquement, $\overline{a}$ étant inversible dans $\mathbb{F}_{q^n}$, $\left(\overline{D^{(i)}}(R)\right)_{i\geq 0} = \left(u_i^{-1}\overline{\Delta^{(i)}}(R)\right)_{i\geq 0}$ et on aboutit de même à la q^n-automaticité de $\left(\overline{D^{(i)}}(R)\right)_{i\geq 0}$.

ANNEXES

Annexe A

Table des polynômes de Bell

$\mathbf{B_{1,1}} = x_1$ $\mathbf{B_{2,1}} = x_2$, $\mathbf{B_{2,2}} = x_1^2$ $\mathbf{B_{3,1}} = x_3^2$, $\mathbf{B_{3,2}} = 3x_1x_2$, $\mathbf{B_{3,3}} = x_1^3$ $\mathbf{B_{4,1}} = x_4$, $\mathbf{B_{4,2}} = 4x_1x_3 + 3x_2^2$, $\mathbf{B_{4,3}} = 6x_1^2 + x_2$, $\mathbf{B_{4,4}} = x_1^4$ $\mathbf{B_{5,1}} = x_5$, $\mathbf{B_{5,2}} = 5x_1x_4 + 10x_2x_3$, $\mathbf{B_{5,3}} = 10x_1^2x_3 + 15x_1x_2^2$, $\mathbf{B_{5,4}} = 10x_1^3x_2$, $\mathbf{B_{5,5}} = x_1^5$ $\mathbf{B_{6,1}} = x_6$, $\mathbf{B_{6,2}} = 6x_1x_5 + 15x_2x_4$, $\mathbf{B_{6,3}} = 15x_1^2x_4 + 60x_1x_2x_3 + 10x_3^2$, $\mathbf{B_{6,4}} = 20x_1^3x_3 + 45x_1^2x_2^2 + 15x_2^3$, $\mathbf{B_{6,5}} = 15x_1^4x_2$, $\mathbf{B_{6,6}} = x_1^6$, $\mathbf{B_{7,1}} = x_7$, $\mathbf{B_{7,2}} = 7x_1x_6 + 21x_2x_5 + 35x_3x_4$, $\mathbf{B_{7,3}} = 21x_1^2x_5 + 105x_1x_2x_4 + 70x_1x_3^2 + 105x_2^2x_3$, $\mathbf{B_{7,4}} = 35x_1^3x_4 + 210x_1^2x_2x_3 + 105x_1^2x_2^3$, $\mathbf{B_{7,5}} = 35x_1^4x_3 + 105x_1^3x_2^2$, $\mathbf{B_{7,6}} = 21x_1^5x_2$, $\mathbf{B_{7,7}} = x_1^7$, $\mathbf{B_{8,1}} = x_8$, $\mathbf{B_{8,2}} = 8x_1x_7 + 28x_2x_6 + 56x_3x_5 + 35x_4^2$, $\mathbf{B_{8,3}} = 28x_1^2x_6 + 168x_1x_2x_5 + 280x_1x_3x_4 + 210x_2^2x_4 + 280x_2x_3^2$, $\mathbf{B_{8,4}} = 56x_1^3x_5 + 420x_1^2x_2x_4 + 280x_1^2x_3^2 + 840x_1x_2^2 + x_3 + 105x_2^4$, $\mathbf{B_{8,5}} = 70x_1^4x_4 + 560x_1^3x_2x_3 + 420x_1^2x_2^3$, $\mathbf{B_{8,6}} = 56x_1^5x_3 + 210x_1^4x_2^2$, $\mathbf{B_{8,7}} = 28x_1^6x_2$, $\mathbf{B_{8,8}} = x_1^8$, $\mathbf{B_{9,1}} = x_9$, $\mathbf{B_{9,2}} = 9x_1x_8 + 36x_2x_7 + 84x_3x_6 + 126x_4x_5$, $\mathbf{B_{9,3}} = 36x_1^2x_7 + 252x_1x_2x_6 + 504x_1x_3x_5 + 378x_2^2x_5 + 315x_1x_4^2 + 1260x_2x_3x_4 + 280x_3^2$, $\mathbf{B_{9,4}} = 84x_1^3x_6 + 756x_1^2x_2x_5 + 1260x_1^2x_3x_4 + 1890x_1x_2^2x_4 + 2520x_1x_2x_3^2 + 1260x_2^3x_3$, $\mathbf{B_{9,5}} = 126x_1^4x_5 + 1260x_1^3x_2x_4 + 840x_1^3x_3^2 + 3780x_1^2x_2^2x_3 + 945x_1x_2^4$, $\mathbf{B_{9,6}} = 126x_1^5x_4 + 1260x_1^4x_2x_3 + 1260x_1^3x_2^3$, $\mathbf{B_{9,7}} = 84x_1^6x_3 + 378x_1^5x_2^2$, $\mathbf{B_{9,8}} = 36x_1^7x_2$, $\mathbf{B_{9,9}} = x_1^9$, $\mathbf{B_{10,1}} = x_10$, $\mathbf{B_{10,2}} = 10x_1x_9 + 45x_2x_8 + 120x_3x_7 + 210x_4x_6 + 126x_5^2$, $\mathbf{B_{10,3}} = 45x_1^2x_8 + 360x_1x_2x_7 + 840x_1x_3x_6 + 630x_2^2x_6 + 1260x_1x_4x_5 + 2520x_2x_3x_5 + 1575x_2x_4^2 + 2100x_3^2x_4$, $\mathbf{B_{10,4}} = 120x_1^3x_7 + 1260x_1^2x_2x_6 + 2520x_1^2x_3x_5 + 3780x_1x_2^2x_5 + 1575x_1^2x_4^2 + 12600x_1x_2x_3x_4 + 3150x_2^3x_4 + 2800x_1x_3 + 6300x_2^2x_3^2$, $\mathbf{B_{10,5}} = 210x_1^4x_6 + 2520x_1^3x_2x_5 + 4200x_1^3x_3x_4 + 9450x_1^2x_2x_4 + 12600x_1^2x_2x_3^2 + 12600x_1x_2^3x_3 + 945x_2^5$, $\mathbf{B_{10,6}} = 252x_1^5x_5 + 3150x_1^4x_2x_4 + 2100x_1^4x_3^2 + 12600x_1^3x_2^2x_3 + 4725x_1^2x_2^4$, $\mathbf{B_{10,7}} = 210x_1^6x_4 + 2520x_1^5x_2x_3 + 3150x_1^4x_2^3$, $\mathbf{B_{10,8}} = 120x_1^7x_3 + 630x_1^6x_2^2$, $\mathbf{B_{10,9}} = 45x_1^8x_2$, $\mathbf{B_{10,10}} = x_1^{10}$, $\mathbf{B_{11,1}} = x_11$, $\mathbf{B_{11,2}} = 11x_1x_10 + 55x_2x_9 + 165x_3x_8 + 330x_4x_7 + 462x_5x_6$, $\mathbf{B_{11,3}} = 55x_1^2x_9 + 495x_1x_2x_8 + 1320x_1x_3x_7 + 990x_2^2x_7 + 2310x_1x_4x_6 + 4620x_2x_3x_6 + 1386x_1x_5^2 + 6930x_2x_4x_5 + 4620x_3^2x_5 + 5775x_3x_4^2$, $\mathbf{B_{11,4}} = 165x_1^3x_8 + 1980x_1^2x_2x_7 + 4620x_1^2x_3x_6 + 6930x_1x_2^2x_6 + 6930x_1^2x_4x_5 + 27720x_1x_2x_3x_5 + 6930x_2^3x_5 + 17325x_1x_2x_4^2 + 23100x_1x_3^2x_4 + 34650x_2^2x_3x_4 + 15400x_2x_3^3$, $\mathbf{B_{11,5}} = 330x_1^4x_7 + 4620x_1^3x_2x_6 + 9240x_1^3x_3x_5 + 20790x_1^2x_2^2x_5 + 5775x_1^3x_4^2 + 69300x_1^2x_2x_3x_4 + 34650x_1x_2^3x_4 + 15400x_1^2x_3^3 + 69300x_1x_2^2x_3^2 + 17325x_2^4x_3$, $\mathbf{B_{11,6}} = 462x_1^5x_6 + 6930x_1^4x_2x_5 + 11550x_1^4x_3x_4 + 34650x_1^3x_2^2x_4 + 46200x_1^3x_2x_3^2 + 69300x_1^3x_2^3x_3 + 10395x_1x_2^5$, $\mathbf{B_{11,7}} = 462x_1^6x_5 + 6930x_1^5x_2x_4 + 4620x_1^5x_3^2 + 34650x_1^4x_2^2x_3 + 17325x_1^3x_2^4$, $\mathbf{B_{11,8}} = 330x_1^7x_4 + 4620x_1^6x_2x_3 + 6930x_1^5x_2^3$, $\mathbf{B_{11,9}} = 165x_1^8x_3 + 990x_1^7x_2^2$, $\mathbf{B_{11,10}} = 55x_1^9x_2$, $\mathbf{B_{11,11}} = x_1^{11}$, $\mathbf{B_{12,1}} = x_12$, $\mathbf{B_{12,2}} = 12x_1x_11 + 66x_2x_10 + 220x_3x_9 + 495x_4x_8 + 792x_5x_7 + 462x_6^2$, $\mathbf{B_{12,3}} = 66x_1^2x_10 +$

$660x_1x_2x_9 + 1980x_1x_3x_8 + 1485x_2^2x_8 + 3960x_1x_4x_7 + 7920x_2x_3x_7 + 5544x_1x_5x_6 +$
$13860x_2x_4x_6 + 9240x_3^2x_6 + 8316x_2x_5^2 + 27720x_3x_4x_5 + 5775x_4^3$, $\mathbf{B_{12,4}} = 220x_1^3x_9 +$
$2970x_1^2x_2x_8 + 7920x_1^2x_3x_7 + 11880x_1x_2^2x_7 + 13860x_1^2x_4x_6 + 55440x_1x_2x_3x_6 + 13860x_2^3x_6 +$
$8316x_1^2x_5^2 + 83160x_1x_2x_4x_5 + 55440x_1x_3^2x_5 + 83160x_2^2x_3x_5 + 69300x_1x_3x_4^2 + 51975x_2^2x_4^2 +$
$138600x_2x_3^2x_4 + 15400x_3^4$, $\mathbf{B_{12,5}} = 495x_1^4x_8 + 7920x_1^3x_2x_7 + 18480x_1^3x_3x_6 + 41580x_1^2x_2^2x_6 +$
$27720x_1^3x_4x_5 + 166320x_1^2x_2x_3x_5 + 83160x_1x_2^3x_5 + 103950x_1^2x_2x_4^2 + 138600x_1^2x_3^2x_4 +$
$415800x_1x_2^2x_3x_4 + 51975x_2^4x_4 + 184800x_1x_2x_3^2 + 138600x_2^3x_3^2$, $\mathbf{B_{12,6}} = 792x_1^5x_7 +$
$13860x_1^4x_2x_6 + 27720x_1^4x_3x_5 + 83160x_1^3x_2^2x_5 + 17325x_1^4x_4^2 + 277200x_1^3x_2x_3x_4 +$
$207900x_1^2x_2^3x_4 + 61600x_1^3x_3^3 + 415800x_1^2x_2^2x_3^2 + 207900x_1x_2^4x_3 + 10395x_2^6$, $\mathbf{B_{12,7}} = 924x_1^6x_6 +$
$16632x_1^5x_2x_5 + 27720x_1^5x_3x_4 + 103950x_1^4x_2^2x_4 + 138600x_1^4x_2x_3^2 + 277200x_1^3x_2^3x_3 + 62370x_1^2x_2^5$,
$\mathbf{B_{12,8}} = 792x_1^7x_5 + 13860x_1^6x_2x_4 + 9240x_1^6x_3^2 + 83160x_1^5x_2^2x_3 + 51975x_1^4x_2^4$, $\mathbf{B_{12,9}} =$
$495x_1^8x_4 + 7920x_1^7x_2x_3 + 13860x_1^6x_2^3$, $\mathbf{B_{12,10}} = 220x_1^9x_3 + 1485x_1^8x_2^2$, $\mathbf{B_{12,11}} = 66x_1^{10}x_2$,
$\mathbf{B_{12,12}} = x_1^{12}$.

Annexe B

Preuve du Lemme de l'Équation Fonctionnelle

Nous dirons que deux éléments G et H sont congrus modulo $(I_A, \deg m)$ si $G - H = \sum_{ij} b_{ij} X^i Y^j$ avec les $b_{ij} \in I_A^r$ pour tous entiers i et j tels que $i + j < m$. Par définition, $I_A^0 = A$.

Lemme B.0.2 *Écrivons* $f_g(X) = \sum_{n=1}^{+\infty} a_n X^n$ *et posons* $n = q^r m$ *où* m *est non divisible par* q. *Alors* $a_n I_A^r \subset A$.

Preuve : Elle s'obtient par récurrence sur r à partir de l'égalité $d_n = b_n + s_1\sigma(d_{n/q}) + ... + s_r\sigma^r(d_{n/q^r})$ en utilisant le fait que $s_i I_A \subset A$ pour $i = 1, 2, ...$

Lemme B.0.3 *Soient* $G(X,Y) \in A[[X,Y]]$, $n = q^r m$ (q *ne divisant pas* m) *et* $l \in \mathbb{N}^*$. *Nous avons :*

$$G(X,Y)^{nq^l} \equiv \left(\sigma^l * G(X^{q^l}, Y^{q^l})\right)^n \pmod{I_A^{r+1}}. \tag{B.1}$$

Preuve : Comme $\sigma(a) \equiv a^q \pmod{I_A}$ pour tout $a \in A$ et comme $p \in I_A$, nous avons

$$G(X,Y)^{q^l} \equiv \left(\sigma^l * G(X^{q^l}, Y^{q^l})\right) \pmod{I_A}.$$

Par récurrence sur r, nous obtenons pour $r = 0, 1, 2, ...$:

$$G(X,Y)^{q^{l+r}} \equiv \left(\sigma^l * G(X^{q^l}, Y^{q^l})\right)^{q^r} \pmod{I_A^{r+1}}$$

et la congruence de l'énoncé en découle directement.

B.1 Partie a

Démontrons la partie a) du Lemme de l'Équation Fonctionnelle.
Nous noterons $F(X,Y)$ à la place de $F_g(X,Y)$ et $f(X)$ à la place de $f_g(X)$.
Décomposons la série $F(X,Y)$ en posant

$$F(X,Y) = F_1(X,Y) + F_2(X,Y) + ...$$

où les $F_i(X,Y)$ sont homogènes de degré i en X,Y. Comme $f(X) \equiv b_1 X \pmod{\deg 2}$, il vient $f^{-1}(X) \equiv b_1^{-1} X \pmod{\deg 2}$ et ainsi $F(X,Y) \equiv X + Y \pmod{\deg 2}$ et $F_1(X,Y)$ a ses coefficients dans A.
Nous allons montrer par récurrence que $F_n(X,Y)$ a ses coefficients dans A pour tout $n = 1, 2, ...$ Supposons que $F_1(X,Y), ..., F_{n-1}(X,Y)$ ont leurs coefficients dans A. Comme $F(X,Y) \equiv 0 \pmod{\deg 1}$, nous avons pour tout $r \geq 2$:

$$(F_1(X,Y) + ... + F_{n-1}(X,Y))^r \equiv (F(X,Y))^r \pmod{\deg n + 1}.$$

Par le lemme précédent, on a pour $i \in \mathbb{N}^*$:

$$F(X,Y)^{q^i n} \equiv \left(\sigma^i * F(X^{q^i}, Y^{q^i})\right)^n \pmod{I_A^{r+1}, \deg n + 1} \tag{B.2}$$

avec $n = q^r m$ et m non divisible par q. Par définition de la série $F(X,Y)$, nous avons :

$$f(F(X,Y)) = f(X) + f(Y) \tag{B.3}$$

et comme σ est un homomorphisme, il vient :

$$\sigma^i * f\left(\sigma^i * F(X,Y)\right) = \sigma^i * f(X) + \sigma^i * f(Y). \tag{B.4}$$

Maintenant, rappelons que $f(X)$ vérifie l'équation fonctionnelle

$$f(X) = g(X) + \sum_{n=1}^{+\infty} s_n \sigma^n * f(X^{q^n}). \tag{B.5}$$

Écrivons $f(X) = \sum_{n=1}^{+\infty} a_n X^n$ et composons à droite les deux membres de l'égalité B.5 par la série $F(X,Y)$. Nous obtenons :

$$f(F(X,Y)) = g(F(X,Y)) + \sum_{i=1}^{+\infty} s_i \sum_{n=1}^{+\infty} \sigma^i(a_n) \left(F(X,Y)\right)^{q^i n}. \tag{B.6}$$

Maintenant, par l'égalité B.2, le lemme B.0.2 et la propriété

$$(I_A^r b \subset I_A \Rightarrow I_A^r \sigma(b) \subset I_A)$$

pour $r \in \mathbb{N}$ et $b \in K$, nous pouvons affirmer que pour tout i et tout n :

$$s_i\sigma^i(a_n)F(X,Y)^{q^i n} \equiv s_i\sigma^i(a_n)\left(\sigma^i * F(X^{q^i},Y^{q^i})\right)^n \pmod{A, \deg n+1}.$$

En utilisant cette congruence dans B.6 et en tenant compte de B.4 et B.5, nous obtenons, modulo $(A, \deg n+1)$, les quatre congruences suivantes :

$$\left.\begin{aligned} f(F(X,Y)) &\equiv g(F(X,Y)) + \sum_{i=1}^{+\infty} s_i \sum_{n=1}^{+\infty} \sigma^i(a_n)\left(\sigma^i * F(X^{q^i},Y^{q^i})\right)^n \\ &\equiv g(F(X,Y)) + \sum_{i=1}^{+\infty} s_i\sigma^i * f\left(\sigma^i * F(X^{q^i},Y^{q^i})\right) \\ &\equiv g(F(X,Y)) + \sum_{i=1}^{+\infty} s_i\left(\sigma^i * f(X^{q^i}) + \sigma^i * f(Y^{q^i})\right) \\ &\equiv g(F(X,Y)) + f(X) + f(Y) - g(X) - g(Y). \end{aligned}\right\} \quad \text{(B.7)}$$

De plus, comme $g(X) \equiv b_1 X \pmod{\deg 2}$ et comme

$$F(X,Y) \equiv F_n(X,Y) \pmod{A, \deg n+1},$$

nous avons

$$g(F(X,Y)) \equiv b_1 F_n(X,Y) \pmod{A, \deg n+1}. \quad \text{(B.8)}$$

De B.8, B.7 et B.3, nous obtenons que

$$b_1 F_n(X,Y) \equiv 0 \pmod{A, \deg n+1},$$

ce qui prouve que $F_n(X,Y)$ est à coefficients dans A car b_1 est inversible dans A et termine la preuve de la partie a)

B.2 Partie b

Pour démontrer la partie b), on procède de la même manière que pour la partie a) :

Lemme B.2.1 *Soit $\alpha(X) \in A[[X]]$, soit $n = q^r m$ avec m non divisible par q et soit $l \in \mathbb{N}^*$. Alors :*

$$\alpha(X)^{nq^l} \equiv \left(\sigma^l * \alpha(X^{q^l})\right)^n \pmod{I_A^{r+1}}.$$

Preuve : On sait que $\sigma(a) \equiv a^q \pmod{I_A}$ pour $a \in A$ et que $p \in I_A$. Donc $\alpha(X)^{q^l} \equiv \sigma^l * \alpha(X^{q^l}) \pmod{I_A}$. Par récurrence, on obtient

$$\alpha(X)^{q^{l+r}} \equiv \left(\sigma^l * \alpha(X^{q^l})\right)^{q^r} \pmod{I_A^{r+1}}.$$

CQFD
Posons $f(X) = f_g(X)$, $\overline{f(X)} = f_{\overline{g}}(X)$ et $\alpha(X) = f^{-1}(\overline{f}(X)) = \sum_i \alpha_i X^i$. On a $f^{-1}(X) \equiv b_1^{-1} X \pmod{\deg 2}$ et $\overline{f}(X) \equiv \overline{b_1} X \pmod{\deg 2}$.
Ainsi $\alpha(X) = f^{-1}(f(X)) \equiv b_1^{-1}\overline{b_1} X \pmod{\deg 2}$ car b_1^{-1} est inversible dans A et $\alpha_1 \in A$.
Montrons par récurrence que les α_i sont dans A :
Supposons que $\alpha_1,...,\alpha_{n-1} \in A$. Comme $f^{-1}(\overline{f}(X)) \equiv 0 \pmod{\deg 1}$, on a :

$$(\alpha_1 X + ... + \alpha_{n-1} X^{n-1})^r \equiv \alpha(X)^r \pmod{\deg n + 1}.$$

Par le lemme B.2.1, pour tout i on a :

$$\alpha(X)^{q^i n} \equiv \left(\sigma^i * \alpha(X^{q^i n})\right)^n \pmod{I_A, \deg n + 1}$$

où $n = q^r m$ avec m non divisible par q. Par définition de $\alpha(X)$:

$$f(\alpha(X)) = \overline{f}(X). \tag{B.9}$$

D'où $\sigma^i * f(\sigma^i * \alpha(X)) = \sigma^i * \overline{f}(X)$. De plus $f(X) = g(X) + \sum_{n=1}^{+\infty} s_n \sigma^n * f(X^{q^n})$. En composant à droite par la série $\alpha(X)$, il vient :

$$\begin{aligned} f(\alpha(X)) &= g(\alpha(X)) + \sum_{n=1}^{+\infty} s_n \sigma^n * f(\alpha(X)^{q^n}) \\ &= g(\alpha(X)) + \sum_{i=1}^{+\infty} s_i \sum_{n=1}^{+\infty} \sigma^i(\alpha_n)(\alpha(X)^{q^n}). \end{aligned}$$

Par le lemme B.2.1 :

$$s_i \sigma^i(\alpha_n)\alpha(X)^{q^i n} \equiv s_i \sigma^i(\alpha_n) \left(\sigma^i * \alpha(X^{q^i})\right)^n \pmod{A, \deg n + 1},$$

d'où les quatre congruences modulo $(A, \deg n + 1)$:

$$\left.\begin{aligned} f(\alpha(X)) &\equiv g(\alpha(X)) + \sum_{i=1}^{+\infty} s_i \sum_{n=1}^{+\infty} \sigma^i(a_n) \left(\sigma^i * \alpha(X^{q^i})\right)^n \\ &\equiv g(\alpha(X)) + \sum_{i=1}^{+\infty} s_i \sigma^i * f\left(\sigma^i * \alpha(X^{q^i})\right) \\ &\equiv g(\alpha(X)) + \sum_{i=1}^{+\infty} s_i \sigma^i * \overline{f}(X^{q^i}) \\ &\equiv g(\alpha(X)) + \overline{f}(X) - \overline{g}(X). \end{aligned}\right\} \tag{B.10}$$

Comme $g(X) \equiv b_1 X \pmod{\deg 2}$ et comme $\alpha(X) \equiv \alpha_1 X + \alpha_2 X^2 + ... + \alpha_n X^n \pmod{A, \deg n+1}$, nous avons

$$g(\alpha(X)) \equiv b_1 \left(\sum_{i=1}^{n} \alpha_i X^i \right) \pmod{A, \deg n+1}. \tag{B.11}$$

Par B.9, B.10, B.11, il vient :

$$b_1 \left(\sum_{i=1}^{n} \alpha_i X^i \right) \equiv 0 \pmod{A, \deg n+1}.$$

L'élément b_1 étant inversible, $\left(\sum_{i=1}^{n} \alpha_i X^i \right) \in A[X]$ et $\alpha_n \in A$.

B.3 Partie c

Posons $\widehat{f}(X) = f(h(X))$. Comme $h(X) \equiv 0 \pmod{A}$, nous avons :

$$\begin{aligned}
&\widehat{f}(X) - \sum_{i=1}^{+\infty} s_i \sigma^i * \widehat{f}(X^{q^i}) \\
&= f(h(X)) - \sum_{i=1}^{+\infty} s_i \sigma^i * f\left(\sigma^i * h(X^{q^i})\right) \\
&= f(h(X)) - \sum_{i=1}^{+\infty} s_i \sum_{n=1}^{+\infty} \sigma^i(a_n) \left(\sigma^i * h(X^{q^i})\right)^n \\
&\equiv f(h(X)) - \sum_{i=1}^{+\infty} s_i \sum_{n=1}^{+\infty} \sigma^i(a_n) \left(h(X)^{q^i n}\right) \pmod{A} \\
&= f(h(X)) - \sum_{i=1}^{+\infty} s_i \sigma^i * f\left(h(X)^{q^i}\right) \\
&= g(h(X)) \\
&\equiv 0 \pmod{A}
\end{aligned}$$

B.4 Partie d

Montrons l'implication $\Rightarrow$.

Nous avons vu que $a_n I_A^t \subset A$ si $f(X) = \sum_{i=1}^{+\infty} a_i X^i$ et $n = q^t m$ avec m non divisible par q. Maintenant si $\beta(X) = \alpha(X) + \gamma(X)$ avec $\gamma(X) \in I_A^r A[[X]]$, il vient comme dans la preuve du lemme B.0.3 :

$$\beta(X)^{q^t} \equiv \alpha(X)^{q^t} \pmod{I_A^{r+t}}$$

et

$$\beta(X)^n \equiv \alpha(X)^n \pmod{I_A^{r+t}}.$$

Donc $a_n\beta(X)^n \equiv a_n\alpha(X)^n \pmod{I_A^r}$, et $f(\alpha(X)) \equiv f(\beta(X)) \pmod{I_A^r}$.

En ce qui concerne l'implication $\Leftarrow$, nous montrons tout d'abord que

$$\alpha(X) \equiv 0 \pmod{I_A^r} \Rightarrow f^{-1}(\alpha(X)) \equiv 0 \pmod{I_A^r}. \tag{B.12}$$

Écrivons $f^{-1}(\alpha(X)) = \gamma(X)$ puis $\alpha(X) = f(\gamma(X))$. Comme $f(X) \equiv b_1 X \pmod{\deg 2}$ avec b_1 inversible dans A, il vient

$$\gamma(X) \equiv 0 \pmod{I_A^r, \deg 2}.$$

Supposons que $\gamma(X) \equiv 0 \pmod{I_A^r, \deg n}$. Comme $\gamma(X)^{q^i} \equiv 0 \pmod{I_A^{r+1}, \deg n + 1}$, nous avons, modulo $(I_A, \deg n + 1)$, les congruences suivantes :

$$\begin{aligned} \alpha(X) &\equiv f(\gamma(X)) = g(\gamma(X)) + \sum_{i=1}^{+\infty} s_i \sigma^i * f\left(\gamma(X)^{q^i}\right) \\ &\equiv 0. \end{aligned}$$

Donc, par l'implication $\Rightarrow$ du d),

$$f\left(\gamma(X)^{q^i}\right) \equiv 0 \pmod{I_A^{r+1}, \deg n + 1},$$

ce qui prouve par récurrence la congruence B.12.
Supposons maintenant que

$$f(\alpha(X)) \equiv f(\beta(X)) \pmod{I_A^r}.$$

Remarquons que ni $f(\alpha(X))$ ni $f(\beta(X))$ n'ont nécessairement leurs coefficients dans A. Soit

$$\delta(X) = f^{-1}\left(f(\beta(X)) - f(\alpha(X))\right).$$

Par B.12, $\delta(X) \equiv 0 \pmod{I_A^r}$. Comme $f(\delta(X)) + f(\alpha(X)) = f(\beta(X))$, alors

$$\beta(X) = f^{-1}(f(\delta(X)) + f(\alpha(X))) = F(\delta(X), \alpha(X))$$

et il vient $\beta(X) \equiv \alpha(X) \pmod{I_A^r}$ car $F(X, Y)$ est à coefficients dans A, $F(0, Y) = Y$ et $\delta(X) \equiv 0 \pmod{I_A^r}$.
Ceci termine la preuve de la partie d) du lemme de l'équation fonctionnelle.

Annexe C

Procédures Maple pour les groupes formels

C.1 Groupes formels sur $\mathbb{Z}$

On pose $\mathcal{F}_p = \{f(T) \in \mathbb{Z}_{(p)}[[T]]; f(T) \equiv pT \pmod{\deg 2}; f(T) \equiv T^p \pmod{p}\}$.
Procédure "modulodeg" :
Paramètres d'entrée :

- Un polynôme P en la variable T
- Un entier $d > 0$

Paramètres de sortie :

- Le polynôme $P \bmod T^d$

```
modulodeg:=proc(P,d)
     local P1;
     P1:=collect(P,T);
     P1:=rem(P1,T^d,T);
end;
```

Procédure "EndomorphismeGF" :
(Cette procédure fait appel à "modulodeg")
Paramètres d'entrée :

- Un polynôme $f \in \mathcal{F}_p$ en la variable T
- Un polynôme $g \in \mathcal{F}_p$ en la variable T
- Un élément $a \in \mathbb{Z}_{(p)}$
- Un entier $n > 0$

• Un nombre premier p

Paramètres de sortie :

• Le développement jusqu'au degré n de l'unique série h à coefficients dans $\mathbb{Z}_{(p)}$ qui vérifie $f \circ h = h \circ g$ et $h \equiv aT \pmod{T^2}$

```
EndomorphismeGF:=proc(f,g,a,n,p)
     local f1,g1,F,r,delta;
     f1:=expand(f);
     g1:=expand(g);
     F:=a*T;
     r:=1;
     while (r<=n) do
          delta:=subs(T=F,f1)-subs(T=g1,F);
          delta:=collect(expand(delta),T);
          delta:=modulodeg(delta,r+2);
          delta:=delta/(p^(r+1)-p);
          delta:=simplify(delta);
          r:=r+1;
          F:=F+delta;
     od;
end;
```

Remarque : Pour obtenir l'expression du logarithme de la loi de groupe formel définie par une série $f(T) \in \mathcal{F}_p$, il suffit d'appeler la procédure $commut(p * T, f, 1, n, p)$. Si l'on désire l'exponentielle, on appelle $commut(f, p * T, 1, n, p)$

Procédure "modulodegXY" :

Paramètres d'entrée :

• Un polynôme P en les variables (X, Y) et à coefficients dans $\mathbb{Z}_{(p)}$

• Un entier $n > 0$

Paramètres de sortie :

• Le polynôme P mod $\deg n$

```
modulodegXY:=proc(P,n)
     local i,PP,PPP;
     PP:=sort(expand(P));
     PPP:=0;
     for i from 1 to nops(PP) do
          if degree(op(i,PP))<n then
               PPP:=PPP+op(i,PP);
          fi;
     od;
     PPP:=sort(PPP);
end;
```

Procédure "GroupeFormel" :
(Cette procédure fait appel à "modulodegXY")
Paramètres d'entrée :

- Un polynôme $f \in \mathcal{F}_p$ en la variable T
- Un polynôme $g \in \mathcal{F}_p$ en la variable T
- Un entier $n > 0$
- Un nombre premier p

Paramètres de sortie :

- Le développement à l'ordre n de l'unique série $F(X,Y)$ à coefficients dans $\mathbb{Z}_{(p)}$ qui vérifie $f(F(X,Y)) = F(g(X), g(Y))$ et $F(X,Y) \equiv X + Y \pmod{\deg 2}$

```
GroupeFormel:=proc(f,g,n,p)
     local f1,g1,F,r,gx,gy,X,Y,delta;
     X:='X';
     Y:='Y';
     F:=X+Y;
     f1:=expand(f);
     g1:=expand(g);
     r:=1;
     while (r<=n) do
          gx:=subs(T=X,g1);
          gy:=subs(T=Y,g1);
          delta:=subs(T=F,f1)-subs(X=gx,Y=gy,F);
          delta:=expand(delta);
          delta:=modulodegXY(delta,r+2);
          delta:=delta/(p^(r+1)-p);
          delta:=simplify(delta);
          r:=r+1;
          F:=F+delta;
     od;
     sort(F);
end;
```

C.2 Groupes formels sur $\mathbb{F}_p[t]$

On pose $\mathcal{F}_t = \{f(T) \in \mathbb{F}_p[t][[T]]; f(T) \equiv tT \pmod{\deg 2}; f(T) \equiv T^p \pmod{t}\}$.
Procédure "AutomrophismeCN" :
(Cette procédure fait appel à "modulodeg")
Paramètres d'entrée :

- Un polynôme $f \in \mathcal{F}_t$ en la variable T
- Un polynôme $g \in \mathcal{F}_t$ en la variable T
- Un élément $a \in \mathbb{F}_p[t]$
- Un entier $n > 0$

Paramètres de sortie :

- Le développement jusqu'au degré n de l'automorphisme $\widetilde{\sigma}_{a^{-1}}^{f}$ du corps de normes de l'extension A.P.F. définie par $f(T)$

```
AutomorphismeCN:=proc(f,g,a,n,p)
     local i,j,n1,F,r,delta,cpt,c,den,num,aux,k,F1,FF,d;
     F:=a*T;
     r:=1;
     while (r<=n) do
          delta:=subs(T=F,f)-subs(T=g,F);
          delta:=collect(expand(delta),T);
          delta:=modulodeg(delta,r+2);
          delta:=delta mod p;
          delta:=delta/(t^(r+1)-t);
          delta:=simplify(delta);
          delta:=delta mod p;
          r:=r+1;
          F:=F+delta;
     od;
     FF:=[];
     d:=degree(F,T);
     for i from 1 to d do
          c:=coeff(F,T^i);
          if c<>0 then
               FF:=[op(FF),c*T^i]
          fi;
     od;
     n1:=nops(FF);
     F1:=0;
     for i from 1 to n1 do
          num:=numer(op(i,FF));
          den:=denom(op(i,FF));
          num:=subs(t=0,num);
          aux:=1;
          k:=subs(t=0,den) mod p;
          k:=k^(p-2) mod p;
          aux:=k;
```

```
                num:=num*aux mod p;
                F1:=F1+num;
                od;
                F1;
end;
```

Annexe D

Endomorphismes du groupe de Cartier

Soit A un anneau de valuation discrète de corps résiduel de cardinal q et soit π une uniformisante de A. Dans [8], Cartier établit qu'il existe un groupe formel de Lubin-Tate sur A, admettant la série

$$\sum_{i=0}^{+\infty} \frac{T^{p^i}}{\pi^i}$$

pour logarithme. Par la suite, on appellera ce groupe formel le groupe de Cartier.
Dans le cas où $A = \mathbb{Z}_p$, $q = p$ et $\pi = p$, on retrouve le groupe formel de Lubin-Tate sur $\mathbb{Z}_p$ dont le logarithme est caractérisé par l'équation fonctionnelle

$$\lambda(T) = T + \frac{1}{p}\lambda(T^p).$$

Par le corollaire 2.1.1, on en déduit qu'un isomorphisme entre ce groupe formel et le groupe multiplicatif est donné par la série

$$\exp \lambda(T) - 1 = \exp \sum_{i=0}^{+\infty} \frac{T^{p^i}}{p^i} - 1.$$

Cette série est en fait l'exponentielle d'Artin-Hasse privée de son terme constant : $E(T) - 1$.
Dans l'état actuel des connaissances, nous ne savons pas si la réduction modulo p de cette série est algébrique sur $\mathbb{F}_p(T)$. Ceci nous place dans le contexte où les méthodes du chapitre 2 ne permettent pas de conclure à la condition nécessaire et suffisante d'algébricité des endomorphismes réduits du groupe de Cartier. Néanmoins, il s'avère que ces endomorphismes ont une forme particulière lorsqu'ils sont issus d'un élément entier. En effet, si $a \in \mathbb{Z}$, alors $[a](T) \in \mathbb{Z}[[T]]$. Ce cas ne se présente a priori pour aucun des autres groupes formels de Lubin-Tate (mis à part le groupe multiplicatif), où pour $a \in \mathbb{Z}$, nous avons en général $[a](T) \in \mathbb{Q}[[T]]$.

Si l'on s'intéresse aux endomorphismes du groupe formel des restrictions au sous-corps faisant intervenir le groupe de Galois μ_2 (voir chapitre 2), on s'aperçoit qu'ils vérifient cette même propriété.

Nous donnons ci-dessous le début d'une table pour quelques valeurs de a lorsque $p = 3$. L'intérêt de cette partie est de se demander si, de même que pour le groupe multiplicatif, les endomorphismes du groupe de Cartier ont une forme récurrente simple, forme qui permettrait éventuellement d'établir la condition nécessaire et suffisante d'algébricité des endomorphismes réduits. Nous pourrions alors étendre l'interprétation p-automatique des groupes formels du chapitre 2 à une infinité d'autres groupes formels, via des isomorphismes de réduction algébrique.

a	Début du développement de $[a](T)$
2	$2T - 2T^3 + 8T^5 - 40T^7 + 170T^9 - 648T^{11} + 1424T^{13} + 9752T^{15}$ $-188608T^{17} + 2027768T^{19} + ...$
3	$3T - 8T^3 + 72T^5 - 840T^7 + 9000T^9 - 88992T^{11} + 658776T^{13} + 1199088T^{15} +$ $199267992T^{17} + 5896183992T^{19} + ...$
4	$4T - 20T^3 + 320T^5 - 6720T^7 + 132260T^9 - 2418240T^{11} + 34606720T^{13}$ $-24590400T^{15} - 26485544960T^{17} + 1511406347200T^{19} + ...$
5	$5T - 40T^3 + 1000T^5 - 33000T^7 + 1029320T^9 - 29908000T^{11} + 691603000T^{13}$ $+2387762000T^{15} - 1169728875000T^{17} + 1086068316630000T^{19} + ...$
6	$6T - 70T^3 + 2520T^5 - 120120T^7 + 5435710T^9 - 229463640T^{11} +$ $7772854320T^{13} - 51706055800T^{15} - 25836332074560T^{17}$ $+3534200230684200T^{19} + ...$
7	$7T - 112T^3 + 5488T^5 - 356720T^7 + 22069040T^9 - 1274730688T^{11}$ $+59362175824T^{13} - 615650787808T^{15} - 353942904566608T^{17}$ $+66836102909107728T^{19} + ...$
8	$8T - 168T^3 + 10752T^5 - 913920T^7 + 74059720T^9 - 5606175232T^{11}$ $+343158731776T^{13} - 5020916572672T^{15} - 34182089635921 92T^{17}$ $+850930138996055552T^{19} + ...$
9	$9T - 240T^3 + 19440T^5 + 2093040T^7 + 215078320T^9 - 20653300080T^{11}$ $+1606864389840T^{13} - 312421116024 00T^{15} - 25273427385946320T^{17}$ $+8014148818172672400T^{19} + ...$
10	$10T - 330T^3 + 33000T^5 - 4389000T^7 + 557567890T^9 - 66207889000T^{11}$ $+6378809074000T^{13} - 1582595554211000T^{15} - 151355886759000000T^{17} + ...$

a	Début du développement de $[a](T)$
1/2	$\frac{1}{2}T + \frac{1}{8}T^3 - \frac{1}{32}T^5 + \frac{15}{256}T^9 - \frac{31}{2048}T^{11} - \frac{33}{8192}T^{13} + \frac{31}{8192}T^{15} + ...$
1/3	$\frac{1}{3}T + \frac{8}{81}T^3 - \frac{8}{729}T^5 - \frac{40}{19683}T^7 + \frac{60040}{1594323}T^9 - \frac{57376}{14348907}T^{11} + \frac{797464}{387420489}T^{13}$ $+\frac{4045616}{10460353203}T^{15} + ...$
1/4	$\frac{1}{4}T + \frac{5}{64}T^3 - \frac{5}{1024}T^5 - \frac{5}{4096}T^7 + \frac{3655}{13072}T^9 - \frac{7015}{4194304}T^{11} - \frac{66005}{67108864}T^{13}$ $+\frac{3025}{134217728}T^{15} + ...$
1/5	$\frac{1}{5}T + \frac{8}{125}T^3 - \frac{8}{3125}T^5 - \frac{56}{78125}T^7 + \frac{43416}{1953125}T^9 - \frac{8416}{9765625}T^{11}$ $-\frac{650648}{1220703125}T^{13} - \frac{774384}{30517578125}T^{15} + ...$
1/6	$\frac{1}{6}T + \frac{35}{648}T^3 - \frac{35}{23328}T^5 - \frac{35}{78732}T^7 + \frac{7552895}{408146688}T^9 - \frac{14753935}{29386561536}T^{11}$ $-\frac{1010248435}{3173748645888}T^{13} - \frac{2312206225}{85691213438976}T^{15} + ...$
1/7	$\frac{1}{7}T + \frac{16}{343}T^3 - \frac{16}{16807}T^5 - \frac{240}{823543}T^7 + \frac{639920}{40353607}T^9 - \frac{628416}{1977326743}T^{11}$ $-\frac{2828624}{13841287201}T^{13} - \frac{103647456}{4747561509943}T^{15} + ...$
1/8	$\frac{1}{8}T + \frac{21}{512}T^3 - \frac{21}{32768}T^5 - \frac{105}{524288}T^7 + \frac{931175}{67108864}T^9 - \frac{1835911}{8589934592}T^{11}$ $-\frac{7626213}{549755813888}T^{13} - \frac{73796177}{4398046511104}T^{15} + ...$
1/9	$\frac{1}{9}T + \frac{80}{2187}T^3 - \frac{80}{177147}T^5 - \frac{6160}{43046721}T^7 + \frac{387079120}{31381059609}T^9 - \frac{382646080}{2541865828329}T^{11}$ $-\frac{60680612080}{617673396283947}T^{13} - \frac{1926967348000}{150094635296999121}T^{15} + ...$
1/10	$\frac{1}{10}T + \frac{33}{1000}T^3 - \frac{33}{100000}T^5 - \frac{33}{312500}T^7 + \frac{5551183}{500000000}T^9 - \frac{2199571}{20000000000}T^{11}$ $-\frac{720718273}{10000000000000}T^{13} - \frac{2478718121}{250000000000000}T^{15} + ...$

a	Début du développement de la restriction $[a]_2(T)$
2	$4T + 8T^2 + 36T^3 + 192T^4 + 904T^5 + 3912T^6 + 12608T^7 - 9344T^8$ $-689916T^9 - 8687296T^{10} + ...$
3	$9T + 48T^2 + 496T^3 + 6192T^4 + 72624T^5 + 798912T^6 + 7378128T^7$ $+31280736T^8 - 889423056T^9 - 36029460816T^{10} + ...$
4	$16T + 160T^2 + 2960T^3 + 66560T^4 + 1429280T^5 + 28937120T^6$ $+503388160T^7 + 4906240000T^8 - 138758589680T^9 - 12030147558400T^{10} + ...$
5	$25T + 400T^2 + 11600T^3 + 410000T^4 + 13933200T^5 + 447425600T^6$ $+12456310000T^7 + 206956980000T^8 - 7089634127600T^9$ $-7089634127600T^{10} + ...$
6	$36T + 840T^2 + 35140T^3 + 1794240T^4 + 88395720T^5 + 4119967880T^6$ $+167223954240T^7 + 4171043990400T^8 - 178948663232220T^9$ $-41404944610411200T^{10} + ...$
7	$49T + 1568T^2 + 89376T^3 + 6223392T^4 + 418989984T^5 + 26705053312T^6$ $+1486089077088T^7 + 51652618342976T^8 - 2769249257050976T^9$ $-909615752498174176T^{10} + ...$
8	$64T + 2688T^2 + 200256T^3 + 18235392T^4 + 1607638144T^5$ $+134235805312T^6 + 9802044571648T^7 + 451560509833216T^8$ $-29892996618408896T^9 - 1319780785352 99T^{10} + ...$
9	$81T + 4320T^2 + 407520T^3 + 47005920T^4 + 5253982560T^5$ $+556369530240T^6 + 51580074978720T^7 + 3036977779262400T^8$ $-244736672009593760T^9 - 13956072966320786 6400T^{10} + ...$
10	$100T + 6600T^2 + 768900T^3 + 109560000T^4 + 15137097800T^5$ $+1981826587400T^6 + 227336189960000T^7 + 16639256709680000T^8$

a	Début du développement de la restriction $[a]_2(T)$
1/2	$\frac{1}{4}T - \frac{1}{8}T^2 - \frac{1}{64}T^3 + \frac{1}{128}T^4 + \frac{61}{1024}T^5 + \frac{1}{2048}T^6 - \frac{47}{4096}T^7 - \frac{61}{16384}T^8 + \frac{279}{65536}T^9 + \frac{1261}{262144}T^{10} + \ldots$
1/3	$\frac{1}{9}T - \frac{16}{243}T^2 + \frac{16}{6561}T^3 + \frac{208}{59049}T^4 + \frac{118736}{4782969}T^5 - \frac{622144}{129140163}T^6 - \frac{3468784}{1162261467}T^7 + \frac{6717344}{31381059609}T^8 + \frac{4341844816}{2541865828329}T^9 + \frac{14004573904}{229876792454961}T^{10} + \ldots$
1/4	$\frac{1}{16}T - \frac{5}{128}T^2 + \frac{15}{4096}T^3 + \frac{45}{32768}T^4 + \frac{14445}{1048576}T^5 - \frac{29635}{8388608}T^6 - \frac{68715}{67108864}T^7 + \frac{208475}{107741824}T^8 + \frac{14347495}{17179869184}T^9 + \frac{48430325}{2748779069440}T^{10} + \ldots$
1/5	$\frac{1}{25}T - \frac{16}{625}T^2 + \frac{48}{15625}T^3 + \frac{48}{78125}T^4 + \frac{688}{78125}T^5 - \frac{611392}{244140625}T^6 - \frac{2666096}{6103515625}T^7 + \frac{16148448}{152587890625}T^8 + \frac{1934721904}{3814697265625}T^9 + \frac{6875676784}{95367431640625}T^{10} + \ldots$
1/6	$\frac{1}{36}T - \frac{35}{1944}T^2 + \frac{1015}{419904}T^3 + \frac{2345}{7558272}T^4 + \frac{29987405}{4897760256}T^5 - \frac{484793645}{264479053824}T^6 - \frac{1026728605}{4760622968832}T^7 + \frac{29988420875}{514147280633856}T^8 + \frac{57538360200055}{166583718925369344}T^9 + \frac{211576211896525}{5997013881313296384}T^{10} + \ldots$
1/7	$\frac{1}{49}T - \frac{32}{2401}T^2 + \frac{32}{16807}T^3 + \frac{992}{5764801}T^4 + \frac{1272416}{282475249}T^5 - \frac{19228288}{13841287201}T^6 - \frac{80129888}{6678223072849}T^7 + \frac{1127958976}{33232930569601}T^8 + \frac{410137242976}{1628413597910449}T^9 + \frac{220221504032}{113988895185373143}T^{10} + \ldots$
1/8	$\frac{1}{64}T - \frac{21}{2048}T^2 + \frac{399}{262144}T^3 + \frac{861}{8388608}T^4 + \frac{3707501}{1073741824}T^5 - \frac{37282259}{34359738368}T^6 - \frac{76900747}{1099511627776}T^7 + \frac{1467376379}{70368744177664}T^8 + \frac{865935712999}{4503599627370496}T^9 + \frac{3302420844821}{288230376151711744}T^{10} + \ldots$
1/9	$\frac{1}{81}T - \frac{160}{19683}T^2 + \frac{5920}{4782969}T^3 + \frac{25120}{387420489}T^4 + \frac{771259040}{282429536481}T^5 - \frac{59645653120}{68630377364883}T^6 - \frac{244403419360}{5555906056555523}T^7 + \frac{18147977268800}{1350851717672992089}T^8 + \frac{1494600464314945 60}{9847709021836112328 81}T^9 + \frac{57575307199963000}{7976644307687250986 3361}T^{10} + \ldots$
1/10	$\frac{1}{100}T - \frac{33}{5000}T^2 + \frac{1023}{1000000000}T^3 + \frac{429}{10000000}T^4 + \frac{177089}{80000000}T^5 - \frac{355415071}{500000000000}T^6 - \frac{724733999}{25000000000000}T^7 + \frac{22529872387}{2500000000000000}T^8 + \frac{30727886102551}{250000000000000000}T^9 + \frac{119226003000621}{2500000000000000000}T^{10} + \ldots$

BIBLIOGRAPHIE

Bibliographie

[1] J.-P. Allouche, *Automates finis en théorie des Nombres*, Expo. Math. **5** (1987) 239-266.

[2] J.-P. Allouche, communication privée.

[3] J.-P. Allouche, *Note sur un article de Sharif et Woodcock*, Séminaire de Théorie des Nombres, Bordeaux, **1** (1989) 163-187.

[4] J.-P. Allouche, *Somme des chiffres et transcendance*, Bull. Soc. Math. Fr. **3** (1982) 279-285.

[5] J.-P. Allouche, M. Mendès France et A.J. van der Poorten, *Indépendance algébrique de certaines séries formelles*, Bull. Soc. Math. Fr. **116** (1988) 449-454.

[6] Y. Amice *Les nombres p-adiques*, Presses Universitaires de France (1975).

[7] C. Cadic *Modules de Drinfeld formels et algébricité*, C.R. Acad. Sc. Paris, t. 327, Série 1 (1998) 335-338.

[8] P. Cartier *Groupes de Lubin-Tate généralisés*, Invent. Math. **35** (1976) 273-284.

[9] G. Christol, *Ensembles presque périodiques k-reconnaissables*, Th. Comp. Sci., t. 9 (1979) 141-145.

[10] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France, **108** (1980), 401-419.

[11] A. Cobham, *On the base-dependence of sets of numbers recognizable by finite automata*, Math. Systems Theory, **3** (1969) 186-192.

[12] A. Cobham, *Uniform tag sequences*, Math. Systems Theory, **6** (1972) 164-192.

[13] L. Comtet *Analyse combinatoire*, Tome Premier, PUF.

[14] P. Deligne, *Intégration sur un cycle évanescent*, Invent. Math., **76** (1983) 129-143.

[15] J. Denef et L. Lipshitz, *Algebraic power series and diagonals*, J. Number Theory **26** (1987) 46-67.

[16] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer (1996).

[17] D. R. Hayes, A brief introduction to Drinfeld modules, in *The Arithmetic of Function Fields*, D. Goss, D. R. Hayes and M. I. Rosen ed., W. de Gruyter (1992) 1-32.

[18] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974) 77-91.

[19] T. Harase, *Algebraic elements in formal power series rings*, Israel J. Math. **63** (1988) 281-288.

[20] T. Harase, *Algebraic elements in formal power series rings II*, Israel J. Math. **67** (1989) 62-66.

[21] M. Hazewinkel, *Formal Groups and Applications*, Academic Press (1978).

[22] Y. Hellegouarch, *Galois Calculus and Carlitz Exponentials*, in *The Arithmetic of Function Fields*, D. Goss, D. R. Hayes and M. I. Rosen ed., W. de Gruyter, 1-32 (1992).

[23] Y. Hellegouarch, *Analogues en caractéristique p d'un théorème de Mason*, C.R. Acad. Sci. Paris, t. 325, Série 1 (1997) 141-144.

[24] K. Iwasawa, *Local Class Field Theory*, Oxford University Press, (1986).

[25] F. Laubie, C. Movahhedi, A. Salinier, *Ramification des polynômes de Chebyshev* (à paraître).

[26] J. Lubin, J. Tate, *Formal Complex Multiplication in Local Fields*, Ann. of Math. **81** (1965) 380-387.

[27] V. Mauduit, *Arithmétique des polynômes selon Carlitz*, Thèse de Doctorat, Université de Caen (1998).

[28] M. Mendès France, A. J. van der Poorten, *Automata and the arithmetic of formal power series*, Acta Arith. **46** (1986) 211-214.

[29] P. Robba, *Sur les équations différentielles linéaires p-adiques (II)*, Pacific J. Math, **98** No. 2 (1982) 393-418.

[30] I. R. Šafarevič, *A general reciprocity law*, Mat. Sb. 26 (68) (1950) 113-146, English transl. in Amer. Math. Soc. Transl. (2) 4 (1956).

[31] J.-P. Serre, *Corps Locaux*, Hermann. Paris (1968).

[32] H. Sharif et C. F. Woodcock, *Algebraic functions over a finite field of positive characteristic and Hadamard products*, J. Lond. Math. Soc. **2** 37 (1988) 396-403.

[33] S. V. Vostokov, *Explicit form of the law of reciprocity*, Math. USSR Izvestija **13** 3 (1979) 557-588.

[34] M. Waldschmidt, *Transcendance problems connected with Drinfeld modules*, Istanbul Univ. Fen Fak. Mat. Der. **49** (1990) 57-75.

[35] J.-P. Wintenberger, *Automorphismes et extensions galoisiennes de corps locaux*, Thèse de $3^{\text{ième}}$ cycle, publication de l'U. S. M. de Grenoble (1978).

[36] J.-P. Wintenberger, *Le corps de normes de certaines extensions infinies de corps locaux*, Applications Ann. Sci. ENS $4^{\text{ième}}$ série 16 (1983) 59-89.

Index

Liste des symboles

U_p	groupe des unités p-adiques,
Λ_n^f	ensemble des α tels que $f^n(\alpha) = 0$,
Λ_∞^f	réunion des Λ_n^f,
$\mathbb{F}_q(t)_P$	complété de $\mathbb{F}_q(t)$ pour la valeur absolue $P(t)$-adique,
$\mathbb{F}_q[t]_P$	anneau de valuation de $\mathbb{F}_q(t)_P$,
Φ	module de Drinfeld,
Φ_R	endomorphisme de Φ vérifiant $\Phi_R \equiv R\sigma^0 \pmod{\sigma}$,
$D^{(i)}(R)$	$i^{\text{ème}}$ dérivée galoisienne de R,
$\Delta^{(i)}(R)$	analogue de $D^{(i)}(R)$ pour les modules de Drinfeld de rang 1,
γ	module de Carlitz,
γ_R	endomorphisme de γ vérifiant $\gamma_R \equiv R\sigma^0 \pmod{\sigma}$,
F_f ou $F_f(X,Y)$	groupe formel de Lubin-Tate admettant $f(T)$ pour endomorphisme,
F ou $F(X,Y)$	groupe formel, éventuellement de Lubin-Tate,
G_m	groupe multiplicatif $X + Y + XY$,
G_a	groupe additif $X + Y$,
$X_K(L)$	corps de normes de L/K,
$A_K(L)$	anneau des entiers de $X_K(L)$,
Y_f	corps de normes $X_K(K(\Lambda_\infty^f))$,
$X_f^{(d)}$	sous-corps du corps de normes $Y_f = X_K(K(\Lambda_\infty^f))$ tel que $Gal(Y_f/X_f^{(d)})$ est isomorphe à μ_d,
X_f	notation "allégée" de $X_f^{(d)}$ lorsque $d = p-1$ (plus grande valeur possible pour d),
$[a]_{fg}(T)$	homomorphisme de F_g dans F_f vérifiant : $[a]_{fg}(T) \equiv aT \pmod{\deg 2}$,
$[a]_{ff}(T)$	endomorphisme du groupe formel F_f vérifiant : $[a]_{ff}(T) \equiv aT \pmod{\deg 2}$,
$\sigma_u^f(T)$ avec $u \in U_p$	automorphisme du groupe de Galois de l'extension maximale abélienne de $\mathbb{Q}_p$ définie par le groupe formel F_f. Cette série est la série $[u^{-1}]_{ff}(T)$,
$\widetilde{\sigma}_u^f(T)$	réduction modulo p de $\sigma_u^f(T)$, automorphisme du corps de normes $X_K(K(\Lambda_\infty^f))$,

$\widetilde{\sigma}_{u,d}^{f}(T)$	restriction de $\widetilde{\sigma}_{u}^{f}(T)$ au sous-corps d'indice d de $X_K(K(\Lambda_\infty^f))$,
$\sigma_{u,d}^{f}(T)$	endomorphisme d'un groupe formel qui n'est pas de Lubin-Tate (groupe formel des restrictions), relèvement de l'automorphisme $\widetilde{\sigma}_{u,d}^{f}(T)$,
$S_\lambda(T)$	série de Chebyshev,
$B_{n,k}$	polynôme de Bell.

Résumé :

Ce travail part de l'observation d'un résultat de P. Robba établi en 1982 dont l'énoncé est le suivant : si λ est un entier p-adique, alors la série $(1+T)^{\lambda} \in \mathbb{Z}_p[[T]]$ réduite modulo p est algébrique sur $\mathbb{F}_p(T)$ si et seulement si $\lambda \in \mathbb{Q}$. En remarquant que cette série a une expression très proche de celle d'un endomorphisme du groupe multiplicatif sur $\mathbb{Z}_p$, on généralise ce résultat à une classe de groupes formels de Lubin-Tate dont le logarithme vérifie une certaine condition d'algébricité. Nous interprétons ensuite ce résultat via le foncteur X_K de Fontaine et Wintenberger et en tirons des conséquences sur l'indépendance algébrique des automorphismes de corps locaux.

Dans la deuxième partie de ce travail, nous établissons l'analogue du théorème de P. Robba dans le cas des modules de Drinfeld de rang 1 définis sur le complété P-adique $\mathbb{F}_q[t]_P$ de $\mathbb{F}_q[t]$ où P est un polynôme irréductible unitaire de $\mathbb{F}_q[t]$ de degré n.

p-automatic interpretation of Lubin-Tate formal groups and reduced Drinfeld modules

Abstract :

This work is firstly based on the observation of a result by P. Robba which states, for any p-adic integer λ, the equivalence between the rationality of λ and the algebraicity of $(1+T)^{\lambda} \bmod p \in \mathbb{F}_p[[T]]$ over $\mathbb{F}_p(T)$. As this power series is, before reduction, essentially the same as the endomorphism $[\lambda]_{ff}(T)$ of the multiplicative group over $\mathbb{Z}_p$, we generalize this result to a class of Lubin-Tate formal groups whose logarithm satisfies a certain condition of algebraicity. Then, we interpret the result by means of the Fontaine-Wintenberger's fonctor X_K and draw consequences about algebraic independence of automorphisms of local fields.

In the second part of this work, we establish the analogue of the Robba's theorem in the context of Drinfeld modules of rank 1 defined on the P-adic completion $\mathbb{F}_q[t]_P$ of $\mathbb{F}_q[t]$, where P is a monic prime polynomial over $\mathbb{F}_q$ with degree n.

Discipline : Mathématiques pures.

Mots-clés : Automate, corps de normes, groupe formel, module de Drinfeld.

UPRESA CNRS 6090, Faculté des sciences de Limoges,
123 avenue Albert Thomas,
87060 Limoges cedex, France.